

US
924

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 2 年 1 1 月 1 5 日
Date of Application:

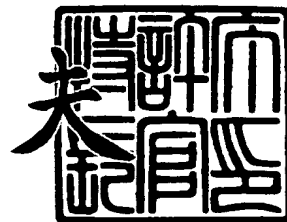
出 願 番 号 特 願 2 0 0 2 - 3 3 2 4 0 4
Application Number:
[ST. 10/C] : [J P 2 0 0 2 - 3 3 2 4 0 4]

出 願 人 日本電気株式会社
Applicant(s): 日本電気通信システム株式会社

2 0 0 3 年 9 月 2 5 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康



出証番号 出証特 2 0 0 3 - 3 0 7 8 9 4 9

【書類名】 特許願

【整理番号】 49200231

【あて先】 特許庁長官殿

【国際特許分類】 H04L 9/08
H04L 12/56
G06F 13/00

【発明者】

【住所又は居所】 東京都港区芝五丁目 7 番 1 号 日本電気株式会社内

【氏名】 鈴木 一哉

【発明者】

【住所又は居所】 東京都港区芝五丁目 7 番 1 号 日本電気株式会社内

【氏名】 地引 昌弘

【発明者】

【住所又は居所】 東京都港区三田一丁目 4 番 2 8 号 日本電気通信システム株式会社内

【氏名】 馬越 英之

【特許出願人】

【識別番号】 000004237

【氏名又は名称】 日本電気株式会社

【特許出願人】

【識別番号】 000232254

【氏名又は名称】 日本電気通信システム株式会社

【代理人】

【識別番号】 100088890

【弁理士】

【氏名又は名称】 河原 純一

【手数料の表示】

【予納台帳番号】 009690

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9001717

【包括委任状番号】 9002497

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 マルチキャスト配信システムにおける鍵交換方式

【特許請求の範囲】

【請求項 1】 暗号化データのマルチキャスト配信が行われるネットワークシステムにおいて、

暗号鍵・復号鍵を作成し、当該暗号鍵・復号鍵とその鍵番号および残り有効時間とを管理し、使用中の鍵の有効時間内に次に使用する復号鍵を鍵管理サーバに配布し、暗号化データとその暗号化で使用した暗号鍵の鍵番号とを有するマルチキャストパケットの送信を行うコンテンツサーバと、

使用中の鍵の有効時間内であって前記コンテンツサーバが前記鍵管理サーバに次に使用する復号鍵を配布した後の時点に前記鍵管理サーバに対して当該次に使用する復号鍵の送付を要求し、前記コンテンツサーバから受信したマルチキャストパケット中の鍵番号に対応する復号鍵によって当該マルチキャストパケット中の暗号化データの復号化を行うクライアントと、

復号鍵とその鍵番号および残り有効時間とを管理し、前記コンテンツサーバから次に使用する復号鍵を受け取り、前記クライアントからの要求に応じて当該次に使用する復号鍵を前記クライアントに送信する前記鍵管理サーバと

を有することを特徴とするマルチキャスト配信システムにおける鍵交換方式。

【請求項 2】 暗号化データのマルチキャスト配信が行われるネットワークシステムにおいて、

暗号鍵とその鍵番号および残り有効時間とを管理し、使用中の鍵の有効時間内に次に使用する暗号鍵・復号鍵の作成を鍵管理サーバに要求し、その要求に応じて作成された暗号鍵を前記鍵管理サーバから取得し、暗号化データとその暗号化で使用した暗号鍵の鍵番号とを有するマルチキャストパケットの送信を行うコンテンツサーバと、

使用中の鍵の有効時間内であって前記コンテンツサーバが前記鍵管理サーバに次に使用する暗号鍵・復号鍵の作成を要求した後の時点に前記鍵管理サーバに対して当該次に使用する復号鍵の送付を要求し、前記コンテンツサーバから受信したマルチキャストパケット中の鍵番号に対応する復号鍵によって当該マルチキャスト

トパケット中の暗号化データの復号化を行うクライアントと、
暗号鍵・復号鍵とその鍵番号および残り有効時間とを管理し、前記コンテンツサーバからの要求に応じて次に使用する暗号鍵・復号鍵を作成・保管し、当該次に使用する暗号鍵を前記コンテンツサーバに送信し、前記クライアントからの要求に応じて当該次に使用する復号鍵を前記クライアントに送信する前記鍵管理サーバと

を有することを特徴とするマルチキャスト配信システムにおける鍵交換方式。

【請求項3】 コンテンツサーバからクライアントに送信されるマルチキャストパケット中の情報に鍵管理サーバのアドレスを加えることによって、クライアント側での復号鍵の問合せ・要求先の設定を不要にすることを特徴とする請求項1または請求項2記載のマルチキャスト配信システムにおける鍵交換方式。

【請求項4】 暗号化データのマルチキャスト配信が行われるネットワークシステムにおいて、

使用中の暗号鍵・復号鍵とその鍵番号とその残り有効時間との組および次に使用する暗号鍵・復号鍵とその鍵番号とその残り有効時間との組を保持するコンテンツサーバ内の鍵情報管理テーブルと、

使用中の鍵の残り有効時間が第1設定値となった時に、鍵管理サーバに対して次に使用する復号鍵に関する鍵情報メッセージを送信し、使用中の鍵の残り有効時間が0となった時に、次に使用する鍵として自テーブルに保持されていた鍵を新しい使用中の鍵に切り替えて、新たな次に使用する暗号鍵・復号鍵を作成してその鍵情報を自テーブルに保存するコンテンツサーバ内の鍵管理手段と、

マルチキャスト配信時に自テーブルに保持されている使用中の暗号鍵を用いて配信データを暗号化し、暗号化データと当該暗号鍵の鍵番号とを有するマルチキャストパケットを送信するコンテンツサーバ内の暗号化・パケット送信手段と、

使用中の復号鍵とその鍵番号とその残り有効時間との組を保持し、次に使用する復号鍵とその鍵番号とその残り有効時間との組を保持しうるクライアント内の鍵情報管理テーブルと、

コンテンツサーバから送信されてきたマルチキャストパケットを受信し、受信したマルチキャストパケット中の鍵番号によって自テーブルから復号鍵を検索し、

その鍵番号の復号鍵によって当該マルチキャストパケット中の暗号化データの復号化を行うクライアント内のパケット受信・復号化手段と、

使用中の鍵の残り有効時間が第2設定値となった時に、鍵管理サーバに対して鍵情報要求を送信し、その返信である応答メッセージ中の次に使用する復号鍵とその鍵番号とその残り有効時間との組を自テーブルに保存し、コンテンツサーバから送信されてくるマルチキャストパケット中の鍵番号の変化の認識に基づいてそれまで次に使用する鍵として自テーブルに保持していた鍵を新しい使用中の鍵に切り替えるクライアント内の鍵管理手段と、

使用中の復号鍵とその鍵番号とその残り有効時間との組を保持し、次に使用する復号鍵とその鍵番号とその残り有効時間との組を保持しうる鍵管理サーバ内の鍵情報管理テーブルと、

コンテンツサーバから受け取った鍵情報メッセージ中の次に使用する復号鍵とその鍵番号とその残り有効時間との組を自テーブルに保存し、使用中の鍵の残り有効時間が第2設定値となった時にクライアントから鍵情報要求を受け取った際に、次に使用する復号鍵とその鍵番号とその残り有効時間との組を含む応答メッセージを当該クライアントに返送し、使用中の鍵の残り有効時間が0となった時に、次に使用する鍵として自テーブルに保持されていた鍵を新しい使用中の鍵に切り替える鍵管理サーバ内の鍵管理手段と

を有することを特徴とするマルチキャスト配信システムにおける鍵交換方式。

【請求項5】 暗号化データのマルチキャスト配信が行われるネットワークシステムにおいて、

使用中の暗号鍵とその鍵番号とその残り有効時間との組を保持し、次に使用する暗号鍵とその鍵番号とその残り有効時間との組を保持しうるコンテンツサーバ内の鍵情報管理テーブルと、

使用中の鍵の残り有効時間が第1設定値となった時に、鍵管理サーバに対して次に使用する鍵の作成を要求する鍵作成要求を発行し、その応答として受け取る鍵情報応答メッセージ中の次に使用する暗号鍵とその鍵番号とその残り有効時間との組を自テーブルに保存し、使用中の鍵の残り有効時間が0となった時に、次に使用する鍵として自テーブルに保持されていた鍵を新しい使用中の鍵に切り替え

るコンテンツサーバ内の鍵管理手段と、

マルチキャスト配信時に自テーブルに保持されている使用中の暗号鍵を用いて配信データを暗号化し、暗号化データと当該暗号鍵の鍵番号とを有するマルチキャストパケットを送信するコンテンツサーバ内の暗号化・パケット送信手段と、

使用中の復号鍵とその鍵番号とその残り有効時間との組を保持し、次に使用する復号鍵とその鍵番号とその残り有効時間との組を保持しうるクライアント内の鍵情報管理テーブルと、

コンテンツサーバから送信されてきたマルチキャストパケットを受信し、受信したマルチキャストパケット中の鍵番号によって自テーブルから復号鍵を検索し、その鍵番号の復号鍵によって当該マルチキャストパケット中の暗号化データの復号化を行うクライアント内のパケット受信・復号化手段と、

使用中の鍵の残り有効時間が第 2 設定値となった時に、鍵管理サーバに対して鍵情報要求を送信し、その返信である応答メッセージ中の次に使用する復号鍵とその鍵番号とその残り有効時間との組を自テーブルに保存し、コンテンツサーバから送信されてくるマルチキャストパケット中の鍵番号の変化の認識に基づいてそれまで次に使用する鍵として自テーブルに保持していた鍵を新しい使用中の鍵に切り替えるクライアント内の鍵管理手段と、

使用中の暗号鍵・復号鍵とその鍵番号とその残り有効時間との組を保持し、次に使用する暗号鍵・復号鍵とその鍵番号とその残り有効時間との組を保持しうる鍵管理サーバ内の鍵情報管理テーブルと、

コンテンツサーバから受け取った鍵作成要求に応じて、次に使用する暗号鍵・復号鍵を作成し、当該次に使用する暗号鍵・復号鍵とその鍵番号とその残り有効時間との組を自テーブルに保存し、当該次に使用する暗号鍵に関する鍵情報応答メッセージをコンテンツサーバに返送し、使用中の鍵の残り有効時間が第 2 設定値となった時にクライアントから鍵情報要求を受け取った際に、次に使用する復号鍵とその鍵番号とその残り有効時間との組を含む応答メッセージを当該クライアントに返送し、使用中の鍵の残り有効時間が 0 となった時に、次に使用する鍵として自テーブルに保持されていた鍵を新しい使用中の鍵に切り替える鍵管理サーバ内の鍵管理手段と

を有することを特徴とするマルチキャスト配信システムにおける鍵交換方式。

【請求項 6】 コンテンツサーバからクライアントに送信されるマルチキャストパケット中の情報に鍵管理サーバのアドレスを加えることによって、クライアント側での鍵情報要求の送信先の設定を不要にすることを特徴とする請求項 4 または請求項 5 記載のマルチキャスト配信システムにおける鍵交換方式。

【請求項 7】 暗号化データのマルチキャスト配信が行われるネットワークシステムにおいて、

コンテンツサーバを、使用中の暗号鍵・復号鍵とその鍵番号とその残り有効時間との組および次に使用する暗号鍵・復号鍵とその鍵番号とその残り有効時間との組を保持する鍵情報管理テーブル、使用中の鍵の残り有効時間が第 1 設定値となった時に、鍵管理サーバに対して次に使用する復号鍵に関する鍵情報メッセージを送信し、使用中の鍵の残り有効時間が 0 となった時に、次に使用する鍵として自テーブルに保持されていた鍵を新しい使用中の鍵に切り替えて、新たな次に使用する暗号鍵・復号鍵を作成してその鍵情報を自テーブルに保存する鍵管理手段、ならびにマルチキャスト配信時に自テーブルに保持されている使用中の暗号鍵を用いて配信データを暗号化し、暗号化データと当該暗号鍵の鍵番号とを有するマルチキャストパケットを送信する暗号化・パケット送信手段として機能させるためのコンテンツサーバ用鍵交換制御プログラムと、

クライアントを、使用中の復号鍵とその鍵番号とその残り有効時間との組を保持し、次に使用する復号鍵とその鍵番号とその残り有効時間との組を保持しうる鍵情報管理テーブル、コンテンツサーバから送信されてきたマルチキャストパケットを受信し、受信したマルチキャストパケット中の鍵番号によって自テーブルから復号鍵を検索し、その鍵番号の復号鍵によって当該マルチキャストパケット中の暗号化データの復号化を行うパケット受信・復号化手段、および使用中の鍵の残り有効時間が第 2 設定値となった時に、鍵管理サーバに対して鍵情報要求を送信し、その返信である応答メッセージ中の次に使用する復号鍵とその鍵番号とその残り有効時間との組を自テーブルに保存し、コンテンツサーバから送信されてくるマルチキャストパケット中の鍵番号の変化の認識に基づいてそれまで次に使用する鍵として自テーブルに保持していた鍵を新しい使用中の鍵に切り替える鍵

管理手段として機能させるためのクライアント用鍵交換制御プログラムと、鍵管理サーバを、使用中の復号鍵とその鍵番号とその残り有効時間との組を保持し、次に使用する復号鍵とその鍵番号とその残り有効時間との組を保持しうる鍵情報管理テーブル、およびコンテンツサーバから受け取った鍵情報メッセージ中の次に使用する復号鍵とその鍵番号とその残り有効時間との組を自テーブルに保存し、使用中の鍵の残り有効時間が第2設定値となった時にクライアントから鍵情報要求を受け取った際に、次に使用する復号鍵とその鍵番号とその残り有効時間との組を含む応答メッセージを当該クライアントに返送し、使用中の鍵の残り有効時間が0となった時に、次に使用する鍵として自テーブルに保持されていた鍵を新しい使用中の鍵に切り替える鍵管理手段として機能させるための鍵管理サーバ用鍵交換制御プログラムと

を有することを特徴とするマルチキャスト配信システムにおける鍵交換方式。

【請求項8】 暗号化データのマルチキャスト配信が行われるネットワークシステムにおいて、

コンテンツサーバを、使用中の暗号鍵とその鍵番号とその残り有効時間との組を保持し、次に使用する暗号鍵とその鍵番号とその残り有効時間との組を保持しうる鍵情報管理テーブル、使用中の鍵の残り有効時間が第1設定値となった時に、鍵管理サーバに対して次に使用する鍵の作成を要求する鍵作成要求を発行し、その応答として受け取る鍵情報応答メッセージ中の次に使用する暗号鍵とその鍵番号とその残り有効時間との組を自テーブルに保存し、使用中の鍵の残り有効時間が0となった時に、次に使用する鍵として自テーブルに保持されていた鍵を新しい使用中の鍵に切り替える鍵管理手段、およびマルチキャスト配信時に自テーブルに保持されている使用中の暗号鍵を用いて配信データを暗号化し、暗号化データと当該暗号鍵の鍵番号とを有するマルチキャストパケットを送信する暗号化・パケット送信手段として機能させるためのコンテンツサーバ用鍵交換制御プログラムと、

クライアントを、使用中の復号鍵とその鍵番号とその残り有効時間との組を保持し、次に使用する復号鍵とその鍵番号とその残り有効時間との組を保持しうる鍵情報管理テーブル、コンテンツサーバから送信されてきたマルチキャストパケッ

トを受信し、受信したマルチキャストパケット中の鍵番号によって自テーブルから復号鍵を検索し、その鍵番号の復号鍵によって当該マルチキャストパケット中の暗号化データの復号化を行うパケット受信・復号化手段、および使用中の鍵の残り有効時間が第2設定値となった時に、鍵管理サーバに対して鍵情報要求を送信し、その返信である応答メッセージ中の次に使用する復号鍵とその鍵番号とその残り有効時間との組を自テーブルに保存し、コンテンツサーバから送信されてくるマルチキャストパケット中の鍵番号の変化の認識に基づいてそれまで次に使用する鍵として自テーブルに保持していた鍵を新しい使用中の鍵に切り替える鍵管理手段として機能させるためのクライアント用鍵交換制御プログラムと、鍵管理サーバを、使用中の暗号鍵・復号鍵とその鍵番号とその残り有効時間との組を保持し、次に使用する暗号鍵・復号鍵とその鍵番号とその残り有効時間との組を保持しうる鍵情報管理テーブル、およびコンテンツサーバから受け取った鍵作成要求に応じて、次に使用する暗号鍵・復号鍵を作成し、当該次に使用する暗号鍵・復号鍵とその鍵番号とその残り有効時間との組を自テーブルに保存し、当該次に使用する暗号鍵に関する鍵情報応答メッセージをコンテンツサーバに返送し、使用中の鍵の残り有効時間が第2設定値となった時にクライアントから鍵情報要求を受け取った際に、次に使用する復号鍵とその鍵番号とその残り有効時間との組を含む応答メッセージを当該クライアントに返送し、使用中の鍵の残り有効時間が0となった時に、次に使用する鍵として自テーブルに保持されていた鍵を新しい使用中の鍵に切り替える鍵管理手段として機能させるための鍵管理サーバ用鍵交換制御プログラムと

を有することを特徴とするマルチキャスト配信システムにおける鍵交換方式。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、マルチキャスト配信時に一定時間毎に異なる鍵によって暗号化を行うことで盗聴を防ぐマルチキャスト配信システムに関し、鍵（暗号鍵／復号鍵）の交換を制御・管理するためのマルチキャスト配信システムにおける鍵交換方式に関する。

【0 0 0'2】**【従来の技術】**

一般に、マルチキャストのパケットは不特定多数の受信者によって受信されるので、特定のクライアントのみに視聴を許可するためには、当該パケットによって配信されるデータに対して暗号鍵による暗号化を施し、視聴を許可したクライアントにのみ復号鍵を配布する必要がある。

【0 0 0 3】

このとき、定期的に鍵を変更することで、クライアントを管理し、さらに暗号の秘匿性を向上させることができる。

【0 0 0 4】

従来より、配信データ（配信対象のデータ）の暗号化が行われるマルチキャスト配信システムにおいては、一定時間毎に異なる鍵によって暗号化を行うことで盗聴を防ぐために、暗号鍵や復号鍵の交換が行われていた（例えば、特許文献 1 参照）。

【0 0 0 5】

このような従来のマルチキャスト配信システムは、コンテンツサーバ（特許文献 1 では「送信部」と表現されている）とクライアント（特許文献 1 では「受信部」と表現されている）と鍵管理サーバとを含んで構成されており、コンテンツサーバが一定時間毎に鍵要求情報を添付したパケットを送信し、それを受けたクライアントが鍵管理サーバに対して鍵を要求することで、一定時間毎に鍵を更新し、鍵が第三者に渡った際にも暗号化データが流出することを防いでいる。

【0 0 0 6】**【特許文献 1】**

特開 2 0 0 1 - 2 8 5 2 7 3 号公報（第 2 - 4 頁、図 1）

【0 0 0 7】**【発明が解決しようとする課題】**

上述した従来のマルチキャスト配信システムにおける鍵交換方式には、次のような問題点があった。

【0 0 0 8】

第 1 の問題点は、鍵要求情報の受信時にタイムラグが生じるという点である。このような問題点が存在する理由は、クライアントが鍵要求情報を受け取った際に、鍵管理サーバに対して鍵を要求しその要求の応答（鍵）を受けてから復号化を開始するため、鍵管理サーバから応答が帰ってくるまでクライアントは暗号化情報（暗号化データ）の復号化ができないからである。

【0 0 0 9】

第 2 の問題点は、放送途中にマルチキャスト放送に参加した場合は即時に視聴することができないという点である。このような問題点が存在する理由は、鍵要求情報が添付されたパケットは一定間隔毎に発生するものであるため、マルチキャスト放送に参加したクライアントは次の鍵要求情報が送られてくるまで復号鍵を取得できず、復号化ができないからである。

【0 0 1 0】

第 3 の問題点は、マルチキャスト配信した鍵要求情報が経路上で消失した際に鍵の取得ができない期間が長期になるおそれがあるという点である。このような問題点が存在する理由は、マルチキャスト配信は応答確認が行われないため、経路上でパケットが消失したことが確認できないので、鍵要求情報を添付したパケットが消失した場合に、次の鍵要求情報が送られてくるまで新しい鍵の取得ができないからである。したがって、新しい鍵が取得できるまで、暗号化情報の復号化ができないようになる。

【0 0 1 1】

本発明の目的は、上述の点に鑑み、以上の問題点を解決し、マルチキャスト配信時に一定時間毎に異なる鍵によって暗号化を行うことで盗聴を防ぐネットワークシステムにおいて、鍵の変更（交換）時の確認遅延（鍵交換遅延）をなくしてリアルタイムのデータの処理を可能にするマルチキャスト配信システムにおける鍵交換方式を提供することにある。

【0 0 1 2】

すなわち、本発明の特徴は、マルチキャスト配信時に配信データを暗号化する場合に、暗号鍵・復号鍵を定期的に変更することによって暗号の秘匿性を向上し、かつ、鍵変更時の新しい鍵情報（鍵およびそれに付随する情報）の取得（クライ

アントによる取得）に伴う遅延を防ぐことを可能にする点にある。

【 0 0 1 3 】

【課題を解決するための手段】

本発明のマルチキャスト配信システムにおける鍵交換方式は、暗号化データのマルチキャスト配信が行われるネットワークシステムにおいて、使用中の暗号鍵・復号鍵（対となる暗号鍵および復号鍵。同じ鍵である場合もある）とその鍵番号（その鍵を識別するための情報）とその残り有効時間との組（その鍵に関する鍵情報）および次に使用する暗号鍵・復号鍵とその鍵番号とその残り有効時間との組を保持するコンテンツサーバ内の鍵情報管理テーブルと、使用中の鍵（暗号鍵・復号鍵）の残り有効時間が第 1 設定値（使用中の鍵の残り有効時間の初期値よりも小さい値であり 0 よりも大きい値）となった時に、鍵管理サーバに対して次に使用する復号鍵に関する鍵情報メッセージ（次に使用する復号鍵とその鍵番号とその残り有効時間との組である鍵情報を有するメッセージ）を送信し、使用中の鍵の残り有効時間が 0 となった時に、次に使用する鍵として自テーブル（コンテンツサーバ内の前記鍵情報管理テーブル）に保持されていた鍵を新しい使用中の鍵に切り替えて、新たな次に使用する暗号鍵・復号鍵を作成してその鍵情報（当該暗号鍵・復号鍵とその鍵番号とその残り有効時間との組）を自テーブルに保存するコンテンツサーバ内の鍵管理手段と、マルチキャスト配信時に自テーブル（コンテンツサーバ内の前記鍵情報管理テーブル）に保持されている使用中の暗号鍵を用いて配信データを暗号化し、暗号化データと当該暗号鍵の鍵番号とを有するマルチキャストパケットを送信するコンテンツサーバ内の暗号化・パケット送信手段と、使用中の復号鍵とその鍵番号とその残り有効時間との組を保持し、次に使用する復号鍵とその鍵番号とその残り有効時間との組を保持しうるクライアント内の鍵情報管理テーブルと、コンテンツサーバから送信されてきたマルチキャストパケットを受信し、受信したマルチキャストパケット中の鍵番号によって自テーブル（自己が存在するクライアント内の前記鍵情報管理テーブル）から復号鍵を検索し、その鍵番号の復号鍵によって当該マルチキャストパケット中の暗号化データの復号化を行うクライアント内のパケット受信・復号化手段と、使用中の鍵の残り有効時間が第 2 設定値（第 1 設定値よりも小さい値であり 0 より

も大きい値) となった時に、鍵管理サーバに対して鍵情報要求を送信し、その返信である応答メッセージ中の次に使用する復号鍵とその鍵番号とその残り有効時間との組を自テーブル（自己が存在するクライアント内の前記鍵情報管理テーブル）に保存し、コンテンツサーバから送信されてくるマルチキャストパケット中の鍵番号の変化の認識に基づいてそれまで次に使用する鍵として自テーブルに保持していた鍵を新しい使用中の鍵に切り替えるクライアント内の鍵管理手段と、使用中の復号鍵とその鍵番号とその残り有効時間との組を保持し、次に使用する復号鍵とその鍵番号とその残り有効時間との組を保持しうる鍵管理サーバ内の鍵情報管理テーブルと、コンテンツサーバから受け取った鍵情報メッセージ中の次に使用する復号鍵とその鍵番号とその残り有効時間との組を自テーブル（鍵管理サーバ内の前記鍵情報管理テーブル）に保存し、使用中の鍵の残り有効時間が第 2 設定値となった時にクライアントから鍵情報要求を受け取った際に、次に使用する復号鍵とその鍵番号とその残り有効時間との組を含む応答メッセージを当該クライアントに返送し、使用中の鍵の残り有効時間が 0 となった時に、次に使用する鍵として自テーブルに保持されていた鍵を新しい使用中の鍵に切り替える鍵管理サーバ内の鍵管理手段とを有する。

【0 0 1 4】

ここで、本発明のマルチキャスト配信システムにおける鍵交換方式は、上記のコンテンツサーバを、上記の鍵情報管理テーブル、鍵管理手段、および暗号化・パケット送信手段として機能させるためのコンテンツサーバ用鍵交換制御プログラムと、上記のクライアントを、上記の鍵情報管理テーブル、パケット受信・復号化手段、および鍵管理手段として機能させるためのクライアント用鍵管理プログラムと、上記の鍵管理サーバを、上記の鍵情報管理テーブルおよび鍵管理手段として機能させるための鍵管理サーバ用鍵交換制御プログラムとを有する態様で実現することも可能である。

【0 0 1 5】

なお、上記の本発明のマルチキャスト配信システムにおける鍵交換方式は、より一般的には、暗号化データのマルチキャスト配信が行われるネットワークシステムにおいて、暗号鍵・復号鍵を作成し、当該暗号鍵・復号鍵とその鍵番号および

残り有効時間とを管理し、使用中の鍵の有効時間内（残り有効時間が0となる前）に次に使用する復号鍵を鍵管理サーバに配布し、暗号化データとその暗号化で使した暗号鍵の鍵番号とを有するマルチキャストパケットの送信を行うコンテンツサーバと、使用中の鍵の有効時間内であって前記コンテンツサーバが前記鍵管理サーバに次に使用する復号鍵を配布した後の時点に前記鍵管理サーバに対して当該次に使用する復号鍵の送付を要求し、前記コンテンツサーバから受信したマルチキャストパケット中の鍵番号に対応する復号鍵によって当該マルチキャストパケット中の暗号化データの復号化を行うクライアントと、復号鍵とその鍵番号および残り有効時間とを管理し、前記コンテンツサーバから次に使用する復号鍵を受け取り、前記クライアントからの要求に応じて当該次に使用する復号鍵を前記クライアントに送信する前記鍵管理サーバとを有すると表現することができる。

【0016】

また、本発明のマルチキャスト配信システムにおける鍵交換方式は、暗号化データのマルチキャスト配信が行われるネットワークシステムにおいて、使用中の暗号鍵とその鍵番号とその残り有効時間との組を保持し、次に使用する暗号鍵とその鍵番号とその残り有効時間との組を保持しうるコンテンツサーバ内の鍵情報管理テーブルと、使用中の鍵の残り有効時間が第1設定値（使用中の鍵の残り有効時間の初期値よりも小さい値であり0よりも大きい値）となった時に、鍵管理サーバに対して次に使用する鍵の作成を要求する鍵作成要求を発行し、その応答として受け取る鍵情報応答メッセージ中の次に使用する暗号鍵とその鍵番号とその残り有効時間との組を自テーブル（コンテンツサーバ内の前記鍵情報管理テーブル）に保存し、使用中の鍵の残り有効時間が0となった時に、次に使用する鍵として自テーブルに保持されていた鍵を新しい使用中の鍵に切り替えるコンテンツサーバ内の鍵管理手段と、マルチキャスト配信時に自テーブル（コンテンツサーバ内の前記鍵情報管理テーブル）に保持されている使用中の暗号鍵を用いて配信データを暗号化し、暗号化データと当該暗号鍵の鍵番号とを有するマルチキャストパケットを送信するコンテンツサーバ内の暗号化・パケット送信手段と、使用中の復号鍵とその鍵番号とその残り有効時間との組を保持し、次に使用する復号

鍵とその鍵番号とその残り有効時間との組を保持しうるクライアント内の鍵情報管理テーブルと、コンテンツサーバから送信されてきたマルチキャストパケットを受信し、受信したマルチキャストパケット中の鍵番号によって自テーブル（自己が存在するクライアント内の前記鍵情報管理テーブル）から復号鍵を検索し、その鍵番号の復号鍵によって当該マルチキャストパケット中の暗号化データの復号化を行うクライアント内のパケット受信・復号化手段と、使用中の鍵の残り有効時間が第2設定値（第1設定値よりも小さい値であり0よりも大きい値）となった時に、鍵管理サーバに対して鍵情報要求を送信し、その返信である応答メッセージ中の次に使用する復号鍵とその鍵番号とその残り有効時間との組を自テーブル（自己が存在するクライアント内の前記鍵情報管理テーブル）に保存し、コンテンツサーバから送信されてくるマルチキャストパケット中の鍵番号の変化の認識に基づいてそれまで次に使用する鍵として自テーブルに保持していた鍵を新しい使用中の鍵に切り替えるクライアント内の鍵管理手段と、使用中の暗号鍵・復号鍵とその鍵番号とその残り有効時間との組を保持し、次に使用する暗号鍵・復号鍵とその鍵番号とその残り有効時間との組を保持しうる鍵管理サーバ内の鍵情報管理テーブルと、コンテンツサーバから受け取った鍵作成要求に応じて、次に使用する暗号鍵・復号鍵を作成し、当該次に使用する暗号鍵・復号鍵とその鍵番号とその残り有効時間との組を自テーブル（鍵管理サーバ内の前記鍵情報管理テーブル）に保存し、当該次に使用する暗号鍵に関する鍵情報応答メッセージ（当該次に使用する暗号鍵とその鍵番号とその残り有効時間との組である鍵情報を有するメッセージ）をコンテンツサーバに返送し、使用中の鍵の残り有効時間が第2設定値となった時にクライアントから鍵情報要求を受け取った際に、次に使用する復号鍵とその鍵番号とその残り有効時間との組を含む応答メッセージを当該クライアントに返送し、使用中の鍵の残り有効時間が0となった時に、次に使用する鍵として自テーブルに保持されていた鍵を新しい使用中の鍵に切り替える鍵管理サーバ内の鍵管理手段とを有するように構成することも可能である。

【0017】

ここで、本発明のマルチキャスト配信システムにおける鍵交換方式は、上記のコンテンツサーバを、上記の鍵情報管理テーブル、鍵管理手段、および暗号化・パ

ケット送信手段として機能させるためのコンテンツサーバ用鍵交換制御プログラムと、上記のクライアントを、上記の鍵情報管理テーブル、パケット受信・復号化手段、および鍵管理手段として機能させるためのクライアント用鍵管理プログラムと、上記の鍵管理サーバを、上記の鍵情報管理テーブルおよび鍵管理手段として機能させるための鍵管理サーバ用鍵交換制御プログラムとを有する態様で実現することも可能である。

【0018】

なお、上記の本発明のマルチキャスト配信システムにおける鍵交換方式は、より一般的には、暗号化データのマルチキャスト配信が行われるネットワークシステムにおいて、暗号鍵とその鍵番号および残り有効時間とを管理し、使用中の鍵の有効時間内に次に使用する暗号鍵・復号鍵の作成を鍵管理サーバに要求し、その要求に応じて作成された暗号鍵を前記鍵管理サーバから取得し、暗号化データとその暗号化で使用した暗号鍵の鍵番号とを有するマルチキャストパケットの送信を行うコンテンツサーバと、使用中の鍵の有効時間内であって前記コンテンツサーバが前記鍵管理サーバに次に使用する暗号鍵・復号鍵の作成を要求した後の時点で前記鍵管理サーバに対して当該次に使用する復号鍵の送付を要求し、前記コンテンツサーバから受信したマルチキャストパケット中の鍵番号に対応する復号鍵によって当該マルチキャストパケット中の暗号化データの復号化を行うクライアントと、暗号鍵・復号鍵とその鍵番号および残り有効時間とを管理し、前記コンテンツサーバからの要求に応じて次に使用する暗号鍵・復号鍵を作成・保管し、当該次に使用する暗号鍵を前記コンテンツサーバに送信し、前記クライアントからの要求に応じて当該次に使用する復号鍵を前記クライアントに送信する前記鍵管理サーバとを有すると表現することができる。

【0019】

さらに、以上列挙した本発明のマルチキャスト配信システムにおける鍵交換方式においては、コンテンツサーバからクライアントに送信されるマルチキャストパケット中の情報に鍵管理サーバのアドレスを加えることによって、クライアント側での鍵情報要求の送信先（復号鍵の問合せ・要求先）の設定を不要にすることも可能である。

【0020】**【発明の実施の形態】**

次に、本発明について図面を参照して詳細に説明する。

【0021】**(1) 第1の実施の形態****【0022】**

図1は、本発明の第1の実施の形態に係るマルチキャスト配信システムにおける鍵交換方式の構成を示すブロック図である。

【0023】

図1を参照すると、本実施の形態に係るマルチキャスト配信システムにおける鍵交換方式は、マルチキャストパケットを送信するコンテンツサーバ11と、コンテンツサーバ11より送られたマルチキャストパケットを受信するクライアント51, 52, ..., 5n (nは正整数)と、コンテンツサーバ11から送られた鍵情報メッセージ71中の復号鍵に関する鍵情報を保管しクライアント5i (iは1～nの正整数)からの鍵情報要求81に対して応答メッセージ82を送信する鍵管理サーバ31と、コンテンツサーバ11, クライアント5i, および鍵管理サーバ31を接続するネットワーク100とを含んで構成されている。

【0024】

コンテンツサーバ11は、マルチキャストパケットによって配信されるデータ(配信データ)の暗号化・復号化に用いる鍵(暗号鍵・復号鍵)とその鍵を識別するための鍵番号とその鍵に対する残り有効時間との組(鍵情報)を保持する鍵情報管理テーブル21を有する(鍵情報管理テーブルは鍵情報を複数保持しうる)。なお、一対の暗号化・復号化処理で用いられる暗号鍵と復号鍵とは、暗号化方式によって、同一である場合も異なる場合もあるが、いずれにしても同一の鍵番号によって識別される。

【0025】

ここで、鍵情報管理テーブル21は、使用中の鍵に関する鍵情報と、次に使用する鍵に関する鍵情報とを保持している。

【0026】

また、コンテンツサーバ 1 1 は、鍵管理手段 1 1 1 と、暗号化・パケット送信手段 1 1 2 とを含んで構成されている。

【0 0 2 7】

鍵管理サーバ 3 1 は、鍵（本実施の形態では、復号鍵）とその鍵を識別するための鍵番号とその鍵に対する残り有効時間との組（鍵情報）を保持する鍵情報管理テーブル 4 1 を有する。

【0 0 2 8】

ここで、鍵情報管理テーブル 4 1 は、使用中の鍵に関する鍵情報を保持しており、次に使用する鍵に関する鍵情報を保持しうる。なお、初期状態では、鍵情報管理テーブル 4 1 は情報を持っていない。

【0 0 2 9】

また、鍵管理サーバ 3 1 は、鍵管理手段 3 1 1 を含んで構成されている。

【0 0 3 0】

クライアント 5 i は、マルチキャストパケットによって配信されるデータの復号化に用いる鍵（復号鍵）とその鍵を識別するための鍵番号とその鍵に対する残り有効時間との組（鍵情報）を保持する鍵情報管理テーブル 6 i を有する。

【0 0 3 1】

ここで、鍵情報管理テーブル 6 i は、使用中の鍵に関する鍵情報を保持しており、次に使用する鍵に関する鍵情報を保持しうる。なお、初期状態では、鍵情報管理テーブル 6 i は情報を持っていない。

【0 0 3 2】

また、クライアント 5 i は、鍵管理手段 5 i 1 と、パケット受信・復号化手段 5 i 2 とを含んで構成されている。

【0 0 3 3】

なお、コンテンツサーバ 1 1，鍵管理サーバ 3 1，および各クライアント 5 i は、それぞれの管理する鍵情報管理テーブル 2 1，鍵情報管理テーブル 4 1，および各鍵情報管理テーブル 6 i 上の鍵情報中の残り有効時間を時間の経過毎に更新する（自己のクロック信号に基づく更新等を行う）。

【0 0 3 4】

図2は、本実施の形態に係るマルチキャスト配信システムにおける鍵交換方式のマルチキャストパケット送受信処理を示す流れ図である。この処理は、配信データ暗号化ステップA1と、マルチキャストパケット送信ステップA2と、マルチキャストパケット受信ステップA3と、使用中鍵番号一致判定ステップA4と、次使用鍵番号一致判定ステップA5と、暗号化データ復号化ステップA6と、鍵管理サーバ問い合わせステップA7とからなる。

【0035】

図3は、本実施の形態に係るマルチキャスト配信システムにおける鍵交換方式の鍵管理に関する処理（使用中の鍵の残り有効時間の値が第1設定値となった時点における処理）を示す流れ図である。この処理は、第1設定値到達認識ステップB1と、鍵情報メッセージ送信ステップB2と、鍵情報メッセージ受信ステップB3と、次使用鍵情報保存ステップB4とからなる。

【0036】

図4は、本実施の形態に係るマルチキャスト配信システムにおける鍵交換方式の鍵管理に関する処理（使用中の鍵の残り有効時間の値が第2設定値となった時点における処理）を示す流れ図である。この処理は、第2設定値到達認識ステップC1と、鍵情報要求送信ステップC2と、鍵情報要求受信ステップC3と、応答メッセージ送信ステップC4と、応答メッセージ受信ステップC5と、次使用鍵情報保存ステップC6とからなる。

【0037】

図5は、本実施の形態に係るマルチキャスト配信システムにおける鍵交換方式の具体的な動作を説明するためのブロック図である。

【0038】

図6は、本実施の形態に係るマルチキャスト配信システムにおける鍵交換方式の具体的な動作を説明するためのシーケンス図である。

【0039】

次に、図1～図6を参照して、上記のように構成された本実施の形態に係るマルチキャスト配信システムにおける鍵交換方式の全体の動作について詳細に説明する。

【0 0 4 0】

第1に、コンテンツサーバ11から各クライアント5iにネットワーク100を介して行われるマルチキャストパケット送受信処理に関する動作について説明する（図2参照）。

【0 0 4 1】

コンテンツサーバ11内の暗号化・パケット送信手段112は、マルチキャスト配信時に、自身が保持している現在使用中の暗号鍵（鍵情報管理テーブル21内の使用中の鍵に関する鍵情報中の暗号鍵）を用いて、配信データ（配信対象のデータ）の暗号化を行う（ステップA1）。

【0 0 4 2】

その上で、暗号化データ（暗号化された配信データ）と当該暗号鍵の鍵番号とを有するマルチキャストパケットをネットワーク100上に送信する（ステップA2）。

【0 0 4 3】

マルチキャストアドレスに参加しているクライアント5i内のパケット受信・復号化手段5i2は、コンテンツサーバ11から送信されたマルチキャストパケットを受信し（ステップA3）、受信したマルチキャストパケットに含まれている暗号化データの復号化処理を行う。

【0 0 4 4】

この復号化処理に際しては、まず、受信したマルチキャストパケット中の鍵番号と自身が記憶している現在使用中の復号鍵の鍵番号（鍵情報管理テーブル6i内の使用中の鍵に関する鍵情報中の鍵番号）とを比較し、両鍵番号が一致するか否かを判定する（ステップA4）。

【0 0 4 5】

ステップA4で「両鍵番号が一致する」と判定した場合には、当該鍵番号の復号鍵を利用して当該マルチキャストパケット中の暗号化データの復号化を行う（ステップA6）。

【0 0 4 6】

一方、ステップA4で「両鍵番号が一致しない」と判定した場合には、当該マル

マルチキャストパケット中の鍵番号と自身が記憶している次に使用する復号鍵の鍵番号（鍵情報管理テーブル 6 i 内の次に使用する鍵に関する鍵情報中の鍵番号）とを比較し、両鍵番号が一致するか否かを判定する（ステップ A 5）。

【0 0 4 7】

ステップ A 5 で「両鍵番号が一致する」と判定した場合には、当該鍵番号の復号鍵を利用して当該マルチキャストパケット中の暗号化データの復号化を行う（ステップ A 6）。

【0 0 4 8】

一方、ステップ A 5 で「両鍵番号が一致しない」と判定した場合（鍵情報管理テーブル 6 i 内に次に使用する鍵に関する鍵情報が存在しない場合を含む）、すなわち、使用中の鍵および次に使用する鍵のどちらの鍵番号についても当該マルチキャストパケット中の鍵番号とは一致しなかった場合には、鍵情報の取得処理が正しく行われていないことを意味するため、鍵管理サーバ 3 1 にその旨の問い合わせを行う（ステップ A 7）。

【0 0 4 9】

第 2 に、使用中の鍵の残り有効時間の値が初期値（残り有効時間初期値）から第 1 設定値（初期値よりも小さい値）までの期間における鍵管理に関する動作について説明する。

【0 0 5 0】

この期間においては、コンテンツサーバ 1 1 内の鍵情報管理テーブル 2 1 は、使用中の鍵（暗号鍵および復号鍵）に関する鍵情報（鍵と鍵番号と残り有効時間との組）と、次に使用する鍵（暗号鍵および復号鍵）に関する鍵情報とを保持している。これらの鍵および鍵番号は、コンテンツサーバ 1 1 内の鍵管理手段 1 1 1 によって作成される。

【0 0 5 1】

また、この期間においては、鍵管理サーバ 3 1 内の鍵情報管理テーブル 4 1 は、使用中の鍵（復号鍵）に関する鍵情報を保持している。

【0 0 5 2】

さらに、この期間においては、各クライアント 5 i 内の鍵情報管理テーブル 6 i

は、使用中の鍵（復号鍵）に関する鍵情報（コンテンツサーバ 1 1 から使用中の鍵によって暗号化されたデータを含むマルチキャストパケットを受信するまでは、次に使用する鍵の鍵情報として管理している）を保持している。また、コンテンツサーバ 1 1 から新たな使用中の鍵によって暗号化されたデータを有するマルチキャストパケットを受信するまでは、直前に使用中の鍵であった鍵に関する鍵情報も保持している。

【0 0 5 3】

なお、この期間に新しくマルチキャストアドレスに参加したクライアント 5 i が存在する場合に、当該クライアント 5 i 内の鍵管理手段 5 i 1 が鍵管理サーバ 3 1 に鍵情報要求 8 1 を送信すると、鍵管理サーバ 3 1 内の鍵管理手段 3 1 1 は使用中の鍵に関する鍵情報を有する応答メッセージ 8 2 を当該クライアント 5 i に送信する。

【0 0 5 4】

第 3 に、使用中の鍵の残り有効時間の値が第 1 設定値となった時点における鍵管理に関する動作について説明する（図 3 参照）。

【0 0 5 5】

コンテンツサーバ 1 1 内の鍵管理手段 1 1 1 は、鍵情報管理テーブル 2 1 で管理している使用中の鍵の残り有効時間の値が第 1 設定値となったこと（残り有効時間の値が減っていった第 1 設定値に達したこと）を認識すると（ステップ B 1）、次に使用する鍵（復号鍵）に関する鍵情報（鍵番号と鍵と残り有効時間との組）を有するメッセージ（鍵情報メッセージ 7 1）を鍵管理サーバ 3 1 に対して送信する（ステップ B 2）。

【0 0 5 6】

鍵管理サーバ 3 1 内の鍵管理手段 3 1 1 は、コンテンツサーバ 1 1 から鍵情報メッセージ 7 1 を受信すると（ステップ B 3）、その鍵情報メッセージ 7 1 中の次に使用する鍵に関する鍵情報を鍵情報管理テーブル 4 1 に保存する（ステップ B 4）。これによって、鍵管理サーバ 3 1 内の鍵情報管理テーブル 4 1 は、使用中の鍵に関する鍵情報と、次に使用する鍵に関する鍵情報とを保持することになる。

【0057】

なお、この時点から使用中の鍵の残り有効時間の値が後述の第2設定値となる時点までの期間において、新しくマルチキャストアドレスに参加したクライアント5*i*が存在する場合に、当該クライアント5*i*内の鍵管理手段5*i*1が鍵管理サーバ31に鍵情報要求81を送信すると、鍵管理サーバ31内の鍵管理手段311は使用中の鍵に関する鍵情報と次に使用する鍵に関する鍵情報とを有する応答メッセージ82を当該クライアント5*i*に送信する。

【0058】

第4に、使用中の鍵の残り有効時間の値が第2設定値（第1設定値よりも小さい値であり0よりも大きい値）となった時点における鍵管理に関する動作について説明する（図4参照）。

【0059】

クライアント5*i*内の鍵管理手段5*i*1は、自身の鍵情報管理テーブル6*i*内の使用中の鍵の残り有効時間の値が第2設定値となった時に、そのこと（残り有効時間の値が減っていった第2設定値に達したこと）を認識し（ステップC1）、次に使用する鍵（復号鍵）に関する鍵情報を得るために、鍵管理サーバ31に対して鍵情報要求81を送信する（ステップC2）。なお、クライアント5*i*には、鍵情報要求81の送信先である鍵管理サーバ31のアドレスが、あらかじめ設定されている。

【0060】

鍵管理サーバ31内の鍵管理手段311は、クライアント5*i*からの鍵情報要求81を受信すると（ステップC3）、その応答として、現在使用中の鍵（復号鍵）に関する鍵情報と次に使用する鍵（復号鍵）に関する鍵情報とを有する応答メッセージ82を当該クライアント5*i*に送信する（ステップC4）。

【0061】

当該クライアント5*i*は、この応答メッセージ82を受信すると（ステップC5）、当該応答メッセージ82中の次に使用する鍵に関する鍵情報を自己の鍵情報管理テーブル6*i*に保存する（ステップC6）。

【0062】

第 5 に、使用中の鍵の残り有効時間の値が 0 となった時点における鍵管理に関する動作について説明する。

【0 0 6 3】

コンテンツサーバ 1 1 内の鍵管理手段 1 1 1 は、鍵情報管理テーブル 2 1 に保持されている使用中の鍵の残り有効時間が 0 となった時に、その使用中の鍵に関する鍵情報を破棄し、次に使用する鍵に関する鍵情報として保持されていた鍵情報を新たな使用中の鍵に関する鍵情報として鍵情報管理テーブル 2 1 に保存する。これにより、暗号化・パケット送信手段 1 1 2 は、その鍵を使用して以後の暗号化処理を行う。

【0 0 6 4】

このときさらに、鍵管理手段 1 1 1 は、新たな次に使用する鍵（暗号鍵および復号鍵）を作成して、その次に使用する鍵に関する鍵情報を鍵情報管理テーブル 2 1 に保存する。

【0 0 6 5】

また、暗号化・パケット送信手段 1 1 2 は、暗号化パケット（暗号化データを有するマルチキャストパケット）に含まれる鍵番号を新たな使用中の鍵に対する鍵番号に変更し、それにより、クライアント 5 i に対して使用中の鍵が変更されたことを示す。

【0 0 6 6】

各クライアント 5 i 内の鍵管理手段 5 i 1 は、コンテンツサーバ 1 1 から送られてきた暗号化パケット（パケット受信・復号化手段 5 i 2 により受信された暗号化パケット）に含まれる鍵番号が変更されたことを確認すると、自身の鍵情報管理テーブル 6 i 内の当該鍵番号を持つ次に使用する鍵を新たな使用中の鍵として保存するようにする。このとき、当該各クライアント 5 i は、新たな次に使用する鍵をまだ得ていないため、自身の鍵情報管理テーブル 6 i において次に使用する鍵に関する鍵情報を持たない状態となる。

【0 0 6 7】

一方、鍵管理サーバ 3 1 内の鍵管理手段 3 1 1 は、鍵情報管理テーブル 4 1 に保持されている使用中の鍵に関する鍵情報中の残り有効時間が 0 となった時に、そ

の使用中の鍵に関する鍵情報を破棄し、次に使用する鍵に関する鍵情報として保持されていた鍵情報を新たな使用中の鍵に関する鍵情報として鍵情報管理テーブル 41 に保存する。このとき、鍵管理サーバ 31 は、新たな次に使用する鍵をまだ得ていないため、鍵情報管理テーブル 41 において次に使用する鍵に関する鍵情報を持たない状態となる。

【0068】

なお、残り有効時間の初期値、第 1 設定値（X とする）および第 2 設定値（Y とする）の設定方法は、例えば、次の a または b に示すような方法が考えられる。

【0069】

a. 当該マルチキャスト配信システム全体で共通な設定値として、手動での設定を行う。

【0070】

b. 鍵の残り有効時間とともにその初期値を各装置（鍵管理サーバおよびクライアント）に送信することで、その初期値から一定の割合の時間を X および Y とし、各装置で求める。この「一定の割合」は、当該マルチキャスト配信システム全体で共通な設定とする。具体例を挙げると、X を鍵の残り有効時間の初期値の 50% とし、Y を鍵の残り有効時間の初期値の 25% とした場合に、鍵の残り有効時間の初期値が 1 時間であった際には、X は 30 分となり、Y は 15 分となる。

【0071】

次に、図 5 および図 6 を参照して、本実施の形態に係るマルチキャスト配信システムにおける鍵交換方式の具体的な動作（一連の動作シーケンス）について説明する。

【0072】

図 5 は、各鍵情報管理テーブル内の情報や、各パケット／要求／メッセージの内容を具体的に示す図である。なお、図 5 においては、使用中の鍵を鍵 A で示しており、次に使用する鍵を鍵 B で示しており、それらの鍵番号を「鍵番号 A」および「鍵番号 B」と表記している。また、この例では、暗号鍵と復号鍵とは同じ鍵であるものとする（例えば、鍵 A は暗号鍵でもあり、復号鍵でもある）。さらに、第 1 設定値を X で示しており、第 2 設定値を Y で示している。

【0 0 7 3】

図 6 は、図 5 に示すような内容の情報が取り扱われる場合の動作シーケンスを時間経過に沿って示した図である。

【0 0 7 4】

この動作シーケンスでは、初期状態（鍵 A の残り有効時間の値が初期値である状態）において、コンテンツサーバ 1 1 は、使用中の鍵の鍵 A と次に使用する鍵の鍵 B とに関する鍵情報を持っている。また、鍵管理サーバ 3 1 およびクライアント 5 1（ここでは、複数のクライアント 5 1 ～ 5 n の中からクライアント 5 1 に注目する）は、図 5 に示す鍵情報のうちの鍵 A に関する鍵情報のみを持っている。なお、残り有効時間の初期値や、X および Y の値は、あらかじめ、コンテンツサーバ 1 1，鍵管理サーバ 3 1，およびクライアント 5 1 ～ 5 n に設定されているものとする。

【0 0 7 5】

鍵 A の残り有効時間の値が X（第 1 設定値）となった時に、コンテンツサーバ 1 1 は、鍵 B（次に使用する鍵）に関する鍵情報を有する鍵情報メッセージ 7 1 を鍵管理サーバ 3 1 に対して送信する。これにより、鍵管理サーバ 3 1 は、図 5 に示すように、鍵 A と鍵 B とに関する鍵情報を持つことになる。

【0 0 7 6】

鍵 A の残り有効時間の値が Y（第 2 設定値）となった時に、クライアント 5 1 は、鍵管理サーバ 3 1 に対して、次に使用する鍵に関する鍵情報を要求する鍵情報要求 8 1 を送信する。

【0 0 7 7】

この鍵情報要求 8 1 を受けた鍵管理サーバ 3 1 は、応答として、現在使用中の鍵（鍵 A）と次に使用する鍵（鍵 B）とに関する鍵情報を有する応答メッセージ 8 2 を送信する。これにより、クライアント 5 1 は、図 5 に示すように、鍵 A と鍵 B とに関する鍵情報を持つことになる。

【0 0 7 8】

鍵 A の残り有効時間の値が 0 となった時に、コンテンツサーバ 1 1 は、使用中の鍵である鍵 A に関する鍵情報を破棄し、保存していた次に使用する鍵である鍵 B

を新たな使用中の鍵として保持し、その鍵 B を使用して配信データの暗号化を行う。また、この時に、コンテンツサーバ 11 は、新たな次に使用する鍵として鍵 C を生成し、この鍵 C に関する鍵情報を鍵情報管理テーブル 21 に保存する。この鍵 C に関する鍵情報は、鍵 B の残り有効時間が X となった時に、鍵情報メッセージ 71 によって、コンテンツサーバ 11 から鍵管理サーバ 31 に対して送信される。

【0079】

鍵管理サーバ 31 は、鍵 A の残り有効時間の値が 0 となった時に、鍵 A に関する鍵情報を破棄し、次に使用する鍵として保存していた鍵 B を現在使用中の鍵として保持する。さらに、コンテンツサーバ 11 からの鍵情報メッセージ 71 によって鍵 C に関する鍵情報を受け取ると、その鍵情報を次に使用する鍵に関する鍵情報として鍵情報管理テーブル 41 に保存する。これにより、鍵情報管理テーブル 41 に保持されている鍵情報は、図 5 中の鍵 A に関する鍵情報が鍵 B に関する鍵情報に入れ替わり、図 5 中の鍵 B に関する鍵情報が鍵 C に関する鍵情報に入れ替わった形となる。

【0080】

クライアント 51 は、コンテンツサーバ 11 から鍵 B の鍵番号を有するマルチキャストパケットを受信すると、鍵 A に関する鍵情報を破棄し、次に使用する鍵として保存していた鍵 B を現在使用中の鍵として保持する。さらに、鍵管理サーバ 31 からの応答メッセージ 82 によって鍵 B の次に使用する鍵である鍵 C に関する鍵情報を受け取ると、その鍵情報を自身の鍵情報管理テーブル 6i に保存する。これにより、当該鍵情報管理テーブル 6i に保持されている鍵情報は、図 5 中の鍵 A に関する鍵情報が鍵 B に関する鍵情報に入れ替わり、図 5 中の鍵 B に関する鍵情報が鍵 C に関する鍵情報に入れ替わった形となる。

【0081】

以上のような動作が繰り返されることによって、クライアント 51（一般的には、各クライアント 5i）は鍵の変更が実行される前に、次に使用する鍵に関する鍵情報を取得することが可能になる。

【0082】

なお、本実施の形態においては、コンテンツサーバ 1 1，鍵管理サーバ 3 1，およびクライアント 5 i の間の通信に掛かる通信遅延は考慮されていない。したがって、そのような通信遅延の分だけ、各鍵情報管理テーブル 2 1，4 1，および 6 i における同一の鍵番号の鍵情報中の残り有効時間の値にずれが生じることも考えられる。このようなずれが実際に問題になる可能性は少ないが、これを考慮する際にも、以下の a および b に示すように、適切な対処が可能となる。

【0083】

a. 使用中の鍵の有効時間が切れる前（残り有効時間が 0 となる前）に次に使用する予定の鍵が使用された暗号化データ（その暗号化データと次に使用する鍵の鍵番号とを有するマルチキャストパケット）がきても、クライアント 5 i は、上記のような構成・動作によって、次に使用する鍵に関する鍵情報を保持しているため、鍵（復号鍵）の特定が可能であり、その復号鍵による解読（復号化）が可能となる。

【0084】

b. 有効時間が切れた後に古い鍵を使用した暗号化データが送られてきたとしても、クライアント 5 i は、残り有効時間が 0 となった後も、新たな使用中の鍵の鍵番号を有するマルチキャストパケットを受信するまでは、古い鍵に関する鍵情報を保持しているので、その鍵（復号鍵）による解読が可能となる。

【0085】

（2） 第 1 の実施の形態の変形形態

【0086】

上記のような第 1 の実施の形態に対しては、コンテンツサーバ 1 1 からクライアント 5 i に配信されるマルチキャストパケットに含まれる情報に関して、以下の a および b に示すような変形形態を考えることができる（a および b を併有する形態も可能である）。

【0087】

a. 上記の第 1 の実施の形態では、マルチキャストパケットは暗号化データと鍵番号とを有していたが、これに対して、さらに、鍵管理サーバ 3 1 のアドレス（アドレスと同様に問合せ先を示す情報を含む）を付加することも可能である。こ

のように、マルチキャストパケット中に鍵管理サーバアドレスを付加して送ることによって、クライアント 5 i 側で鍵情報の問合せ・要求先（鍵情報要求 8 1 の送信先）の設定を不要にすることができる。

【0088】

b. また、マルチキャストパケットには、そのマルチキャストパケットが有している鍵番号で識別される鍵の残り有効時間を付加することも可能である。

【0089】

(3) 第2の実施の形態

【0090】

図7は、本発明の第2の実施の形態に係るマルチキャスト配信システムにおける鍵交換方式の構成を示すブロック図である。

【0091】

図7を参照すると、本実施の形態に係るマルチキャスト配信システムにおける鍵交換方式は、マルチキャストパケットを送信するコンテンツサーバ12と、コンテンツサーバ12より送られたマルチキャストパケットを受信するクライアント51, 52, ..., 5n (nは正整数) と、コンテンツサーバ12から送られた鍵作成要求91に応じて鍵（暗号鍵および復号鍵）を作成・保管して当該暗号鍵とその鍵を識別するための鍵番号とその鍵に対する残り有効時間との組（鍵情報）を有する鍵情報応答メッセージ92をコンテンツサーバ12に返送し、クライアント5i (iは1～nの正整数) からの鍵情報要求81に対して応答メッセージ82を送信する鍵管理サーバ32と、コンテンツサーバ12, クライアント5i, および鍵管理サーバ32を接続するネットワーク100とを含んで構成されている。

【0092】

コンテンツサーバ12は、マルチキャストパケットによって配信されるデータの暗号化に用いる鍵（暗号鍵）とその鍵を識別するための鍵番号とその鍵に対する残り有効時間との組（鍵情報）を保持する鍵情報管理テーブル22を有する（鍵情報管理テーブルは鍵情報を複数保持しうる）。

【0093】

ここで、鍵情報管理テーブル 2 2 は、使用中の鍵に関する鍵情報を保持しており、次に使用する鍵に関する鍵情報を保持しうる。

【0094】

また、コンテンツサーバ 1 2 は、鍵管理手段 1 2 1 と、暗号化・パケット送信手段 1 2 2 とを含んで構成されている。

【0095】

鍵管理サーバ 3 2 は、鍵（暗号鍵・復号鍵）とその鍵を識別するための鍵番号とその鍵に対する残り有効時間との組（鍵情報）を保持する鍵情報管理テーブル 4 2 を有する。なお、本実施の形態では、鍵管理サーバ 3 2 によって鍵の作成が行われるので、鍵管理サーバ 3 2 の鍵情報管理テーブル 4 2 が暗号鍵と復号鍵とに関する鍵情報を保持している。

【0096】

ここで、鍵情報管理テーブル 4 2 は、使用中の鍵に関する鍵情報と、次に使用する鍵に関する鍵情報とを保持している。

【0097】

また、鍵管理サーバ 3 2 は、鍵管理手段 3 2 1 を含んで構成されている。

【0098】

クライアント 5 i は、マルチキャストパケットによって配信されるデータの復号化に用いる鍵（復号鍵）とその鍵を識別するための鍵番号とその鍵に対する残り有効時間との組（鍵情報）を保持する鍵情報管理テーブル 6 i を有する。

【0099】

ここで、鍵情報管理テーブル 6 i は、使用中の鍵に関する鍵情報を保持しており、次に使用する鍵に関する鍵情報を保持しうる。なお、初期状態では、鍵情報管理テーブル 6 i は情報を持っていない。

【0100】

また、クライアント 5 i は、鍵管理手段 5 i 1 と、パケット受信・復号化手段 5 i 2 とを含んで構成されている。

【0101】

なお、コンテンツサーバ 1 2、鍵管理サーバ 3 2、および各クライアント 5 i は

、それぞれの管理する鍵情報管理テーブル 2 2，鍵情報管理テーブル 4 2，および各鍵情報管理テーブル 6 i 上の鍵情報中の残り有効時間を時間の経過毎に更新する（自己のクロック信号に基づく更新等を行う）。

【0 1 0 2】

本実施の形態に係るマルチキャスト配信システムにおける鍵交換方式は、第 1 の実施の形態と比較して、コンテンツサーバ 1 2 が鍵管理サーバ 3 2 に対して鍵作成要求 9 1 を送信し、それに応じて、鍵管理サーバ 3 2 が鍵（暗号鍵・復号鍵）を作成し、作成した暗号鍵に関する鍵情報を有する鍵情報応答メッセージ 9 2 をコンテンツサーバ 1 2 に対して返送する点が異なっている。

【0 1 0 3】

図 8 は、本実施の形態に係るマルチキャスト配信システムにおける鍵交換方式の鍵管理に関する処理（使用中の鍵の残り有効時間の値が第 1 設定値となった時点における処理）を示す流れ図である。この処理は、第 1 設定値到達認識ステップ D 1 と、鍵作成要求送信ステップ D 2 と、鍵作成要求受信ステップ D 3 と、次使用鍵作成ステップ D 4 と、次使用鍵情報保存ステップ D 5 と、鍵情報応答メッセージ送信ステップ D 6 と、鍵情報応答メッセージ受信ステップ D 7 と、次使用鍵情報保存ステップ D 8 とからなる。

【0 1 0 4】

次に、図 7 および図 8 を参照して（図 1 ～図 4 も適宜参照する）、上記のように構成された本実施の形態に係るマルチキャスト配信システムにおける鍵交換方式の動作について、第 1 の実施の形態とは異なる点を中心にして説明する。

【0 1 0 5】

第 1 に、コンテンツサーバ 1 2 から各クライアント 5 i にネットワーク 1 0 0 を介して行われるマルチキャストパケット送受信処理に関する動作について説明する。

【0 1 0 6】

この動作は、第 1 の実施の形態における動作（図 1 中のコンテンツサーバ 1 1 から各クライアント 5 i にネットワーク 1 0 0 を介して行われるマルチキャストパケット送受信処理に関する動作）と同様なものとなる。

【0 1 0 7】

第 2 に、使用中の鍵の残り有効時間の値が初期値から第 1 設定値（初期値よりも小さい値）までの期間における鍵管理に関する動作について説明する。

【0 1 0 8】

この期間においては、コンテンツサーバ 1 2 内の鍵情報管理テーブル 2 2 は、使用中の鍵（暗号鍵）に関する鍵情報（鍵と鍵番号と残り有効時間との組）を保持している。これらの鍵および鍵番号は、鍵管理サーバ 3 2 内の鍵管理手段 3 2 1 によって作成されたものである。

【0 1 0 9】

また、この期間においては、鍵管理サーバ 3 2 内の鍵情報管理テーブル 4 2 は、使用中の鍵（暗号鍵・復号鍵）に関する鍵情報（鍵と鍵番号と残り有効時間との組）を保持している。これらの鍵および鍵番号は、鍵管理サーバ 3 2 内の鍵管理手段 3 2 1 によって作成されたものである。

【0 1 1 0】

なお、上記以外の動作は、第 1 の実施の形態における動作と同様なものとなる。

【0 1 1 1】

第 3 に、使用中の鍵の残り有効時間の値が第 1 設定値となった時点における鍵管理に関する動作について説明する（図 8 参照）。

【0 1 1 2】

第 1 の実施の形態では、コンテンツサーバ 1 1 は、使用中の鍵の残り有効時間の値が第 1 設定値となったことを認識すると、鍵情報メッセージ 7 1 を鍵管理サーバ 3 1 に送信していた。

【0 1 1 3】

これに対して、本実施の形態では、コンテンツサーバ 1 2 内の鍵管理手段 1 2 1 は、鍵情報管理テーブル 2 2 で管理している使用中の鍵の残り有効時間の値が第 1 設定値となったこと（その時点に達したこと）を認識すると（ステップ D 1）、次に使用する鍵（暗号鍵）の鍵情報を得るために、鍵作成要求 9 1 を鍵管理サーバ 3 2 に対して送信する（ステップ D 2）。

【0 1 1 4】

鍵管理サーバ 3 2 内の鍵管理手段 3 2 1 は、コンテンツサーバ 1 2 から鍵作成要求 9 1 を受信すると（ステップ D 3）、その鍵作成要求 9 1 に応じて、次に使用する鍵（暗号鍵・復号鍵）を作成し（ステップ D 4）、その鍵に関する鍵情報（鍵と鍵番号と残り有効時間との組）を鍵情報管理テーブル 4 2 に保存する（ステップ D 5）。これによって、鍵管理サーバ 3 2 内の鍵情報管理テーブル 4 2 は、使用中の鍵に関する鍵情報と、次に使用する鍵に関する鍵情報とを保持することになる。

【0 1 1 5】

さらに、鍵管理手段 3 2 1 は、ステップ D 4 で作成した暗号鍵に関する鍵情報（暗号鍵と鍵番号と残り有効時間との組）を有する鍵情報応答メッセージ 9 2 をコンテンツサーバ 1 2 に送信（返送）する（ステップ D 6）。

【0 1 1 6】

コンテンツサーバ 1 2 内の鍵管理手段 1 2 1 は、鍵管理サーバ 3 2 から鍵情報応答メッセージ 9 2 を受信すると（ステップ D 7）、その鍵情報応答メッセージ 9 2 中の次に使用する鍵（暗号鍵）に関する鍵情報を鍵情報管理テーブル 2 2 に保存する（ステップ D 8）。これによって、コンテンツサーバ 1 2 内の鍵情報管理テーブル 2 2 は、使用中の鍵に関する鍵情報と、次に使用する鍵に関する鍵情報とを保持することになる。

【0 1 1 7】

なお、上記以外の動作は、第 1 の実施の形態における動作と同様なものとなる。

【0 1 1 8】

第 4 に、使用中の鍵の残り有効時間の値が第 2 設定値（第 1 設定値よりも小さい値であり 0 よりも大きい値）となった時点における鍵管理に関する動作について説明する。

【0 1 1 9】

この動作は、第 1 の実施の形態における動作と同様なものとなる。

【0 1 2 0】

第 5 に、使用中の鍵の残り有効時間の値が 0 となった時点における鍵管理に関する動作について説明する。

【0 1 2 1】

コンテンツサーバ 1 2 内の鍵管理手段 1 2 1 は、鍵情報管理テーブル 2 2 に保持されている使用中の鍵の残り有効時間が 0 となった時に、その使用中の鍵に関する鍵情報を破棄し、次に使用する鍵に関する鍵情報として保持されていた鍵情報を新たな使用中の鍵に関する鍵情報として鍵情報管理テーブル 2 2 に保存する。このとき、コンテンツサーバ 1 2 は、新たな次に使用する鍵をまだ得ていないため、鍵情報管理テーブル 2 2 において次に使用する鍵に関する鍵情報を持たない状態となる。

【0 1 2 2】

これにより、暗号化・パケット送信手段 1 2 2 は、その鍵（暗号鍵）を使用して以後の暗号化処理を行う。

【0 1 2 3】

なお、上記以外の動作は、第 1 の実施の形態における動作と同様なものとなる。

【0 1 2 4】

前述の第 1 の実施の形態では、コンテンツサーバ 1 1 と鍵管理サーバ 3 1 との間の通信に障害が発生した際に、鍵（復号鍵）の配布ができなくなることがあった。これに対して、本実施の形態（第 2 の実施の形態）では、コンテンツサーバ 1 2 と鍵管理サーバ 3 2 との間の通信に障害が発生した際にも、以前の鍵を使い続けることで、暗号化データを有するマルチキャストパケットの通信を続けることが可能になる。

【0 1 2 5】

このように、本発明では、上記の第 1 の実施の形態と第 2 の実施の形態とに示すように、鍵をコンテンツサーバで作成する構成も、鍵管理サーバで作成する構成も、実現することが可能である。

【0 1 2 6】

（４） 第 2 の実施の形態の変形形態

【0 1 2 7】

上記の第 2 の実施の形態に対しても、（２）の a および b で述べた第 1 の実施の形態に対する変形形態と同様の変形形態を考えることができる。

【0128】

(5) 第3の実施の形態

【0129】

図9は、本発明の第3の実施の形態に係るマルチキャスト配信システムにおける鍵交換方式の構成を示すブロック図である。

【0130】

図9を参照すると、本発明の第3の実施の形態に係るマルチキャスト配信システムにおける鍵交換方式は、図1に示した第1の実施の形態に係るマルチキャスト配信システムにおける鍵交換方式に対して、コンテンツサーバ用鍵交換制御プログラム901、鍵管理サーバ用鍵交換制御プログラム902、およびクライアント用鍵交換制御プログラム903を備える点が異なっている。

【0131】

コンテンツサーバ用鍵交換制御プログラム901は、コンテンツサーバ11に読み込まれ、当該コンテンツサーバ11の動作を鍵情報管理テーブル21、鍵管理手段111、および暗号化・パケット送信手段112として制御する。コンテンツサーバ用鍵交換制御プログラム901の制御によるコンテンツサーバ11の動作（鍵情報管理テーブル21、鍵管理手段111、および暗号化・パケット送信手段112に関する動作）は、第1の実施の形態におけるコンテンツサーバ11の動作と全く同様になるので、その詳しい説明を割愛する。

【0132】

また、鍵管理サーバ用鍵交換制御プログラム902は、鍵管理サーバ31に読み込まれ、当該鍵管理サーバ31の動作を鍵情報管理テーブル41および鍵管理手段311として制御する。鍵管理サーバ用鍵交換制御プログラム902の制御による鍵管理サーバ31の動作（鍵情報管理テーブル41および鍵管理手段311に関する動作）は、第1の実施の形態における鍵管理サーバ31の動作と全く同様になるので、その詳しい説明を割愛する。

【0133】

さらに、クライアント用鍵交換制御プログラム903は、各クライアント5iに読み込まれ、当該各クライアント5iの動作を鍵情報管理テーブル6i、鍵管理

手段 5 i 1, およびパケット受信・復号化手段 5 i 2 として制御する。クライアント用鍵交換制御プログラム 903 の制御による各クライアント 5 i の動作 (鍵情報管理テーブル 6 i, 鍵管理手段 5 i 1, およびパケット受信・復号化手段 5 i 2 に関する動作) は、第 1 の実施の形態におけるクライアント 5 i の動作と全く同様になるので、その詳しい説明を割愛する。

【0134】

(6) 第 4 の実施の形態

【0135】

図 10 は、本発明の第 4 の実施の形態に係るマルチキャスト配信システムにおける鍵交換方式の構成を示すブロック図である。

【0136】

図 10 を参照すると、本発明の第 4 の実施の形態に係るマルチキャスト配信システムにおける鍵交換方式は、図 7 に示した第 2 の実施の形態に係るマルチキャスト配信システムにおける鍵交換方式に対して、コンテンツサーバ用鍵交換制御プログラム 1001, 鍵管理サーバ用鍵交換制御プログラム 1002, およびクライアント用鍵交換制御プログラム 1003 を備える点が異なっている。

【0137】

コンテンツサーバ用鍵交換制御プログラム 1001 は、コンテンツサーバ 12 に読み込まれ、当該コンテンツサーバ 12 の動作を鍵情報管理テーブル 22, 鍵管理手段 121, および暗号化・パケット送信手段 122 として制御する。コンテンツサーバ用鍵交換制御プログラム 1001 の制御によるコンテンツサーバ 12 の動作 (鍵情報管理テーブル 22, 鍵管理手段 121, および暗号化・パケット送信手段 122 に関する動作) は、第 2 の実施の形態におけるコンテンツサーバ 12 の動作と全く同様になるので、その詳しい説明を割愛する。

【0138】

また、鍵管理サーバ用鍵交換制御プログラム 1002 は、鍵管理サーバ 32 に読み込まれ、当該鍵管理サーバ 32 の動作を鍵情報管理テーブル 42 および鍵管理手段 321 として制御する。鍵管理サーバ用鍵交換制御プログラム 1002 の制御による鍵管理サーバ 32 の動作 (鍵情報管理テーブル 42 および鍵管理手段 3

(2 1 に関する動作) は、第 2 の実施の形態における鍵管理サーバ 3 2 の動作と全く同様になるので、その詳しい説明を割愛する。

【 0 1 3 9 】

さらに、クライアント用鍵交換制御プログラム 1 0 0 3 は、各クライアント 5 i に読み込まれ、当該各クライアント 5 i の動作を鍵情報管理テーブル 6 i , 鍵管理手段 5 i 1 , およびパケット受信・復号化手段 5 i 2 として制御する。クライアント用鍵交換制御プログラム 1 0 0 3 の制御による各クライアント 5 i の動作 (鍵情報管理テーブル 6 i , 鍵管理手段 5 i 1 , およびパケット受信・復号化手段 5 i 2 に関する動作) は、第 2 の実施の形態におけるクライアント 5 i の動作と全く同様になるので、その詳しい説明を割愛する。

【 0 1 4 0 】

【発明の効果】

以上説明したように、本発明によると、以下に示すような効果が生じる。

【 0 1 4 1 】

第 1 の効果は、鍵の変更時に新しい鍵の取得のための遅延が発生しないことにある。すなわち、鍵交換遅延のないマルチキャスト配信時の鍵の変更が可能になるということである。このような効果が生じる理由は、鍵自体とともに鍵番号および鍵の残り有効時間を有する鍵情報を管理し、クライアントが使用中の鍵の有効期間内に次に使用する鍵をあらかじめ取得することができるようにすることにより、鍵を交換した際に即時に新しい鍵を用いて復号化を行うことができるためである。

【 0 1 4 2 】

第 2 の効果は、クライアントがどのマルチキャストアドレスに参加する際でも鍵を要求する鍵管理サーバのアドレスを当該クライアントに設定する必要がなくなることにある。このような効果が生じる理由は、コンテンツサーバが送信するマルチキャストパケットに鍵管理サーバのアドレスを含めることができるため、クライアントはその鍵管理サーバアドレスに対して鍵の要求を行うことができるからである。

【 0 1 4 3 】

第 3 の効果は、視聴者（クライアント）の情報を正確にリアルタイムに取得することにある。このような効果が生じる理由は、本発明を用いることで鍵変更時の遅延がなくなるため、通信遅延を増大させずに鍵の変更サイクルを短くすることができ、クライアントの情報を鍵管理サーバで集計するサイクル（クライアントが復号化のために所定時間毎に鍵管理サーバに対して行う鍵取得の要求の際に当該クライアントの情報を鍵管理サーバで集計するサイクル）も短くでき、より正確なクライアントの情報を取得することができるからである。

【0 1 4 4】

第 4 の効果は、「暗号化によって視聴者（クライアント）を限定し、許可しない相手が情報を取得することを防ぐ」という暗号化方式による利点を、より確実に実現することができることにある。このような効果が生じる理由は、上記のように本発明では鍵を一定時間毎に変更することを効率的に実現できるため、万一鍵が漏れたとしても、鍵の変更により不正者が連続して視聴することを防ぐことができるからである。また、復号化に必要な鍵を管理する鍵管理サーバに視聴を許可する相手または許可しない相手を設定することで、復号鍵を渡す相手を特定することができるからでもある。

【図面の簡単な説明】

【図 1】

本発明の第 1 の実施の形態に係るマルチキャスト配信システムにおける鍵交換方式の構成を示すブロック図である。

【図 2】

図 1 に示すマルチキャスト配信システムにおける鍵交換方式のマルチキャストパケット送受信処理を示す流れ図である。

【図 3】

図 1 に示すマルチキャスト配信システムにおける鍵交換方式の鍵管理に関する処理（使用中の鍵の残り有効時間の値が第 1 設定値となった時点における処理）を示す流れ図である。

【図 4】

図 1 に示すマルチキャスト配信システムにおける鍵交換方式の鍵管理に関する処

(I)

理（使用中の鍵の残り有効時間の値が第 2 設定値となった時点における処理）を示す流れ図である。

【図 5】

図 1 に示すマルチキャスト配信システムにおける鍵交換方式の具体的な動作を説明するためのブロック図である。

【図 6】

図 1 に示すマルチキャスト配信システムにおける鍵交換方式の具体的な動作を説明するためのシーケンス図である。

【図 7】

本発明の第 2 の実施の形態に係るマルチキャスト配信システムにおける鍵交換方式の構成を示すブロック図である。

【図 8】

図 7 に示すマルチキャスト配信システムにおける鍵交換方式の鍵管理に関する処理（使用中の鍵の残り有効時間の値が第 1 設定値となった時点における処理）を示す流れ図である。

【図 9】

本発明の第 3 の実施の形態に係るマルチキャスト配信システムにおける鍵交換方式の構成を示すブロック図である。

【図 1 0】

本発明の第 4 の実施の形態に係るマルチキャスト配信システムにおける鍵交換方式の構成を示すブロック図である。

【符号の説明】

1 1, 1 2 コンテンツサーバ

2 1, 2 2, 4 1, 4 2, 6 1, 6 2, …, 6 n 鍵情報管理テーブル

3 1, 3 2 鍵管理サーバ

5 1, 5 2, …, 5 n クライアント

7 1 鍵情報メッセージ

8 1 鍵情報要求

8 2 応答メッセージ

9 1 鍵作成要求

9 2 鍵情報応答メッセージ

1 0 0 ネットワーク

1 1 1, 1 2 1, 3 1 1, 3 2 1, 5 1 1, 5 2 1, ..., 5 n 1 鍵管理手段

1 1 2, 1 2 2 暗号化・パケット送信手段

5 1 2, 5 2 2, ..., 5 n 2 パケット受信・復号化手段

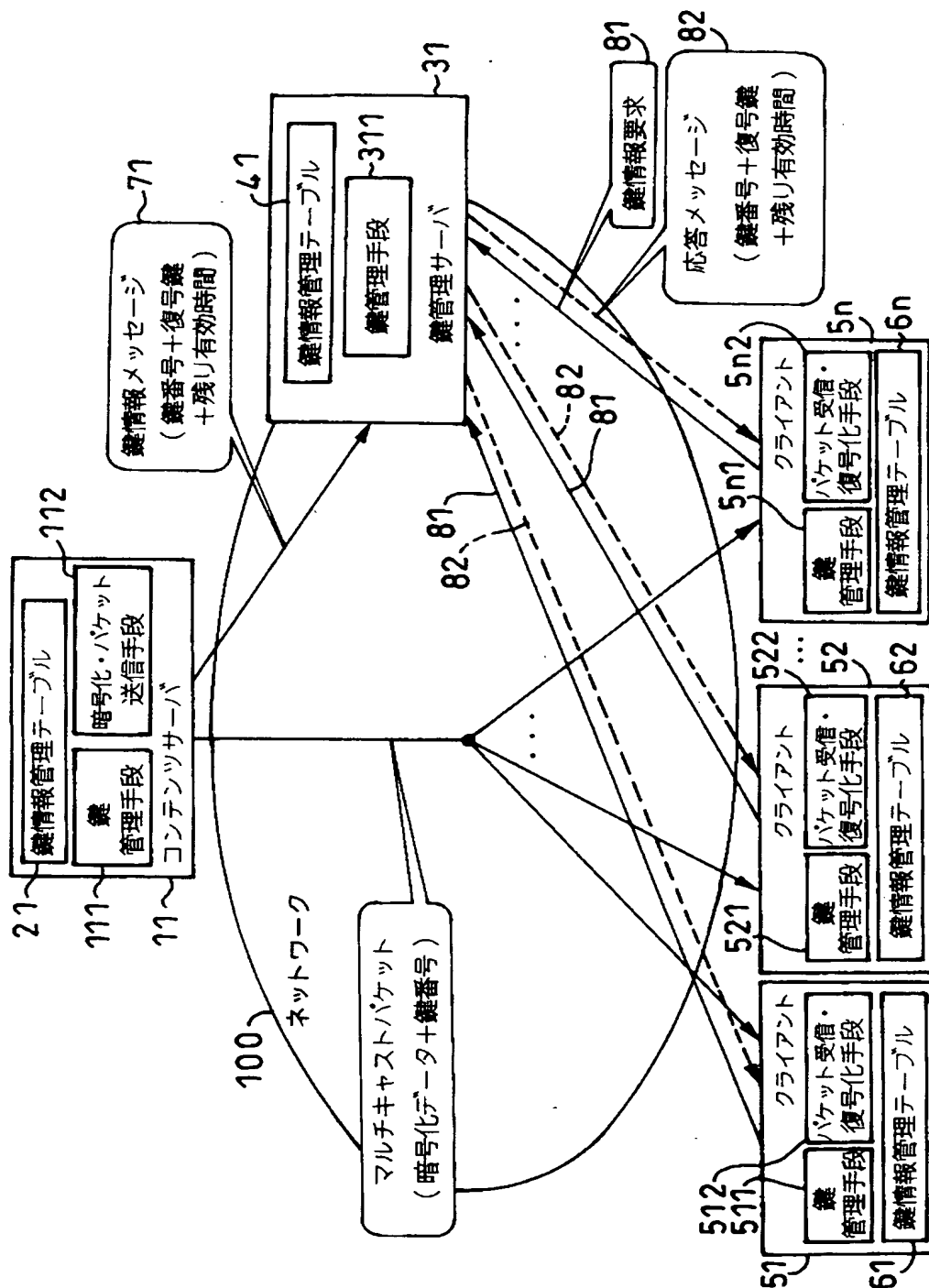
9 0 1, 1 0 0 1 コンテンツサーバ用鍵交換制御プログラム

9 0 2, 1 0 0 2 鍵管理サーバ用鍵交換制御プログラム

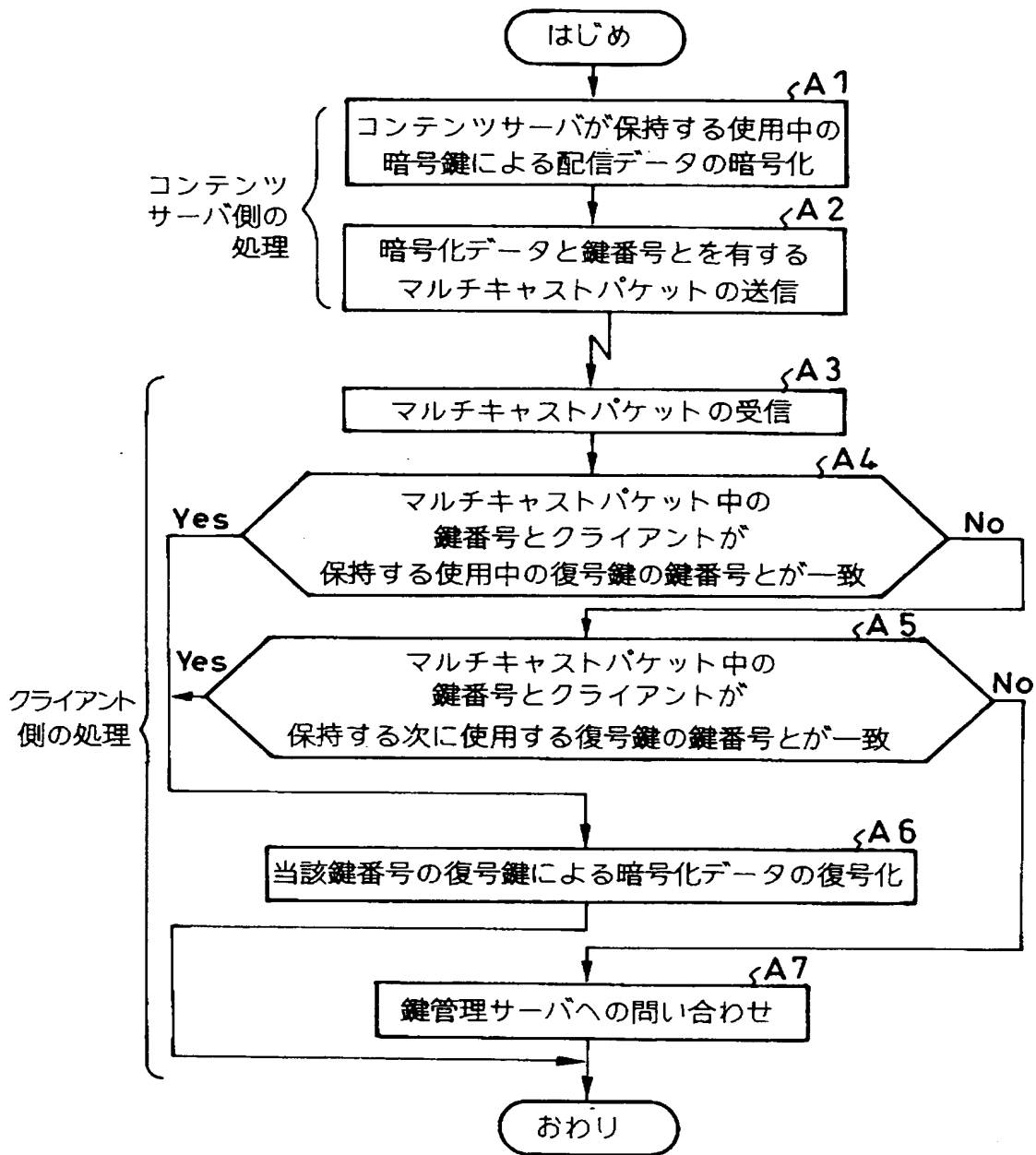
9 0 3, 1 0 0 3 クライアント用鍵交換制御プログラム

【書類名】 図面

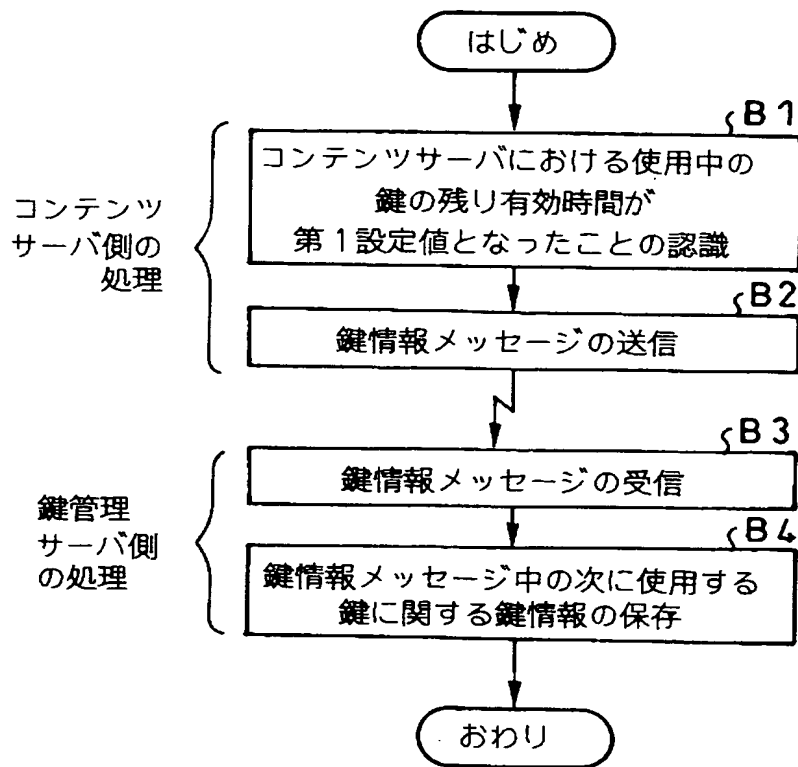
【図 1】



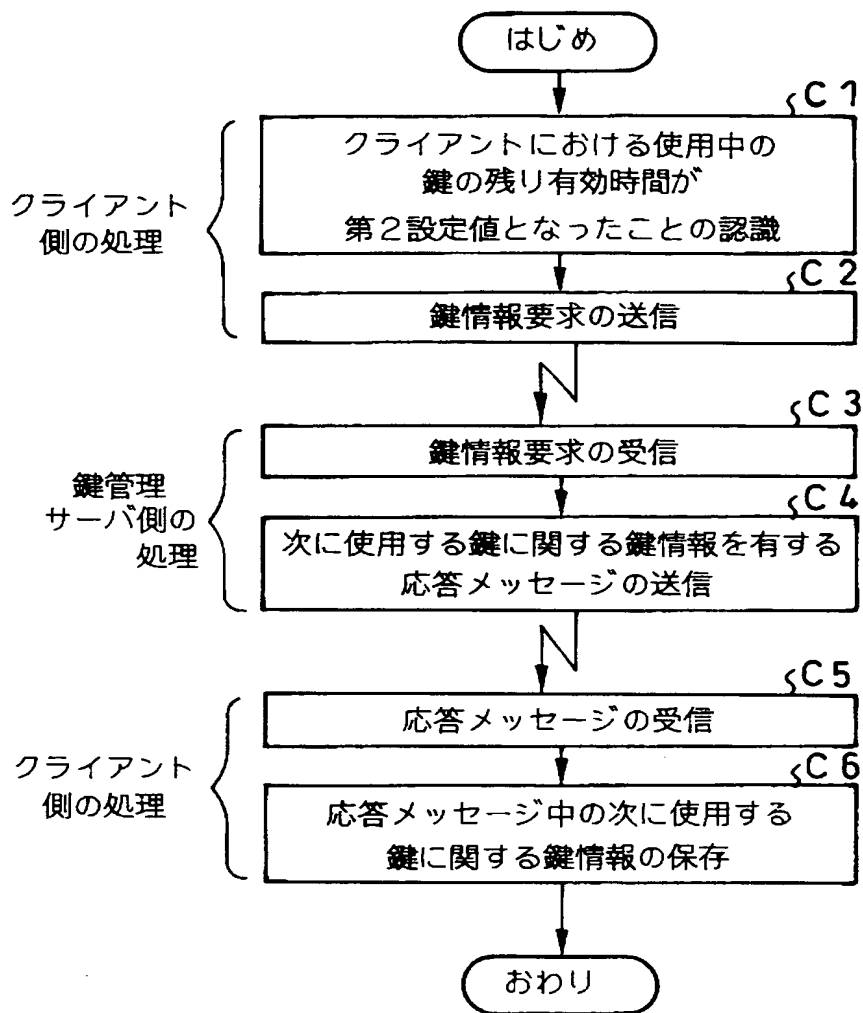
【図 2】



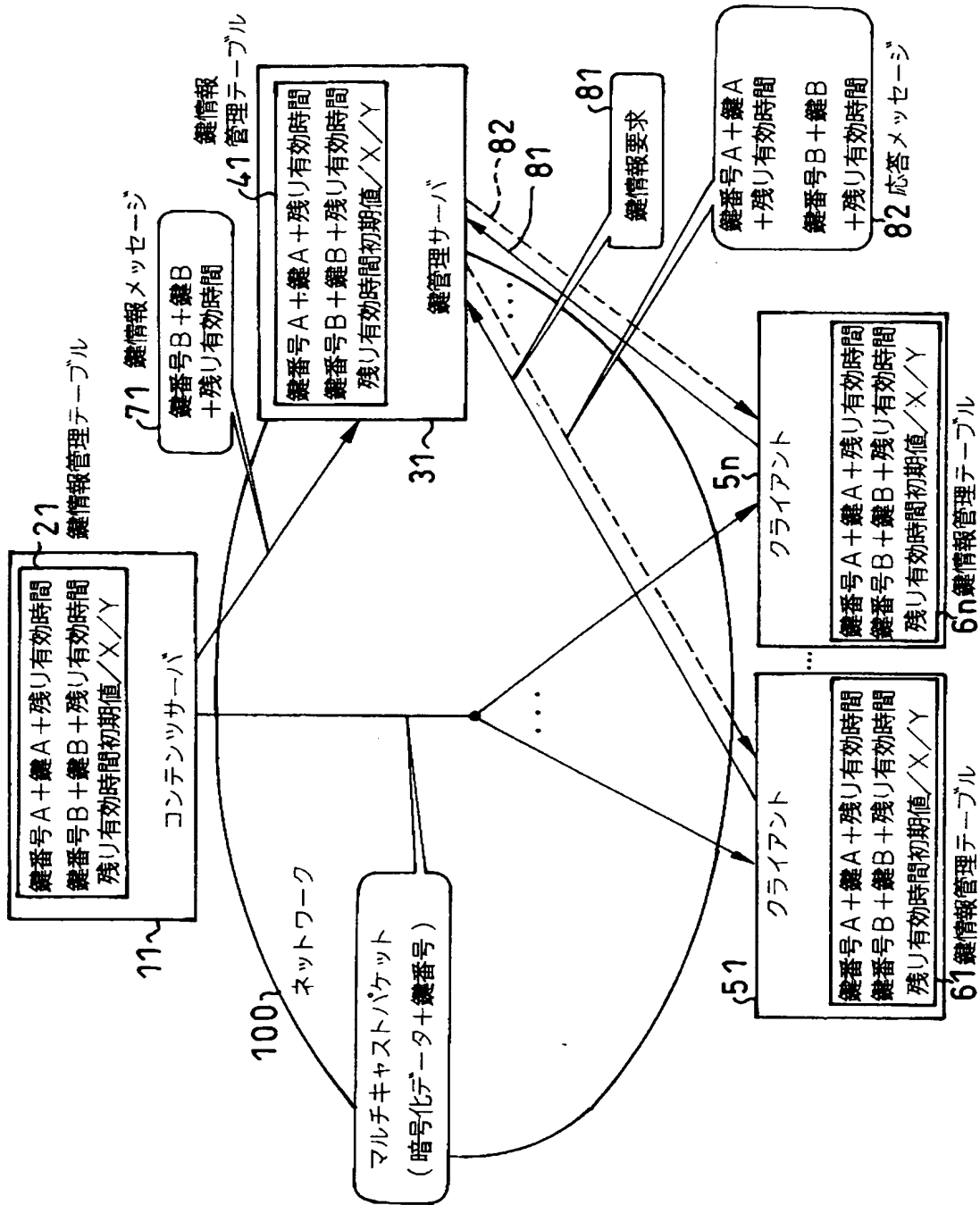
【図 3】



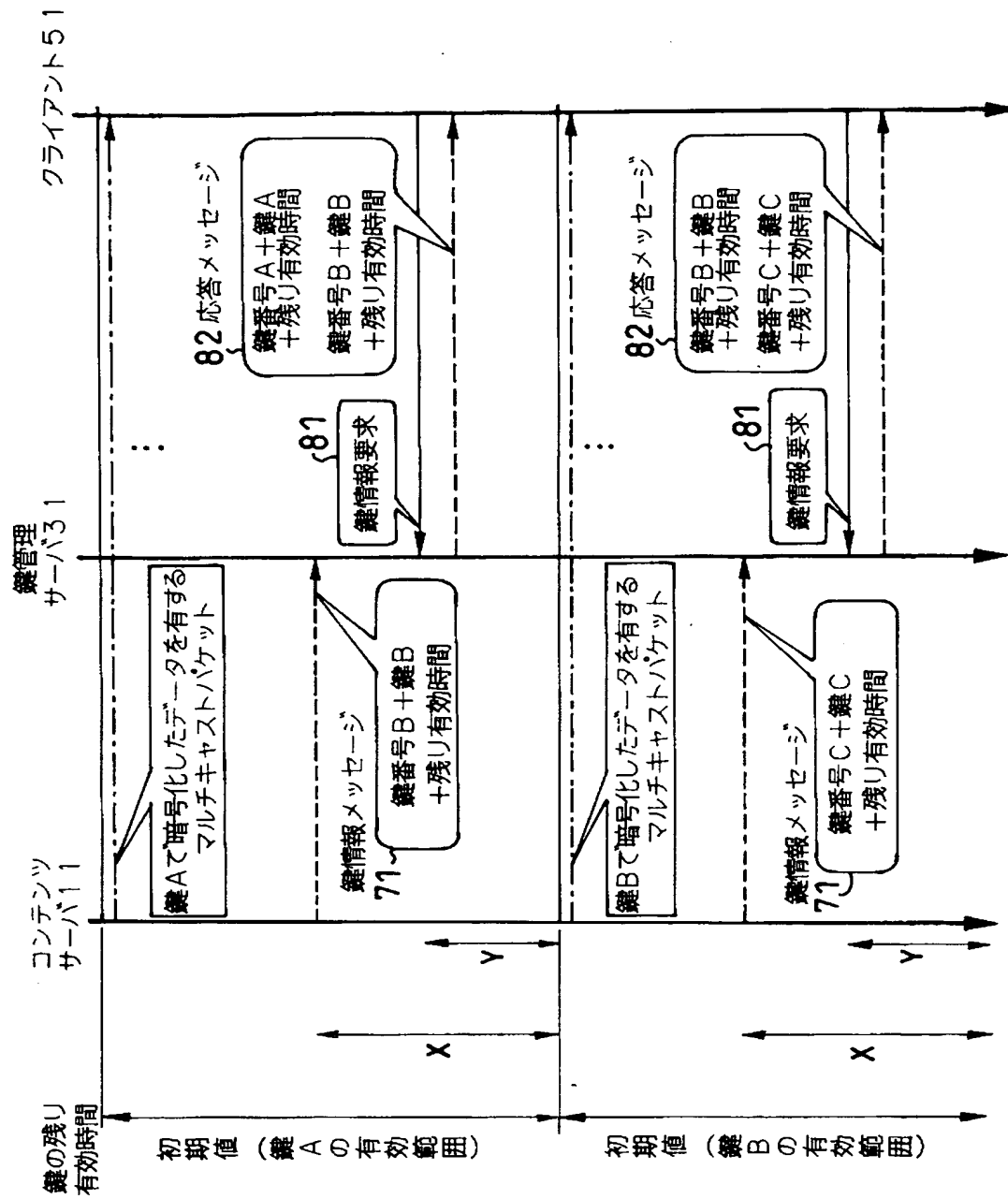
【図 4】



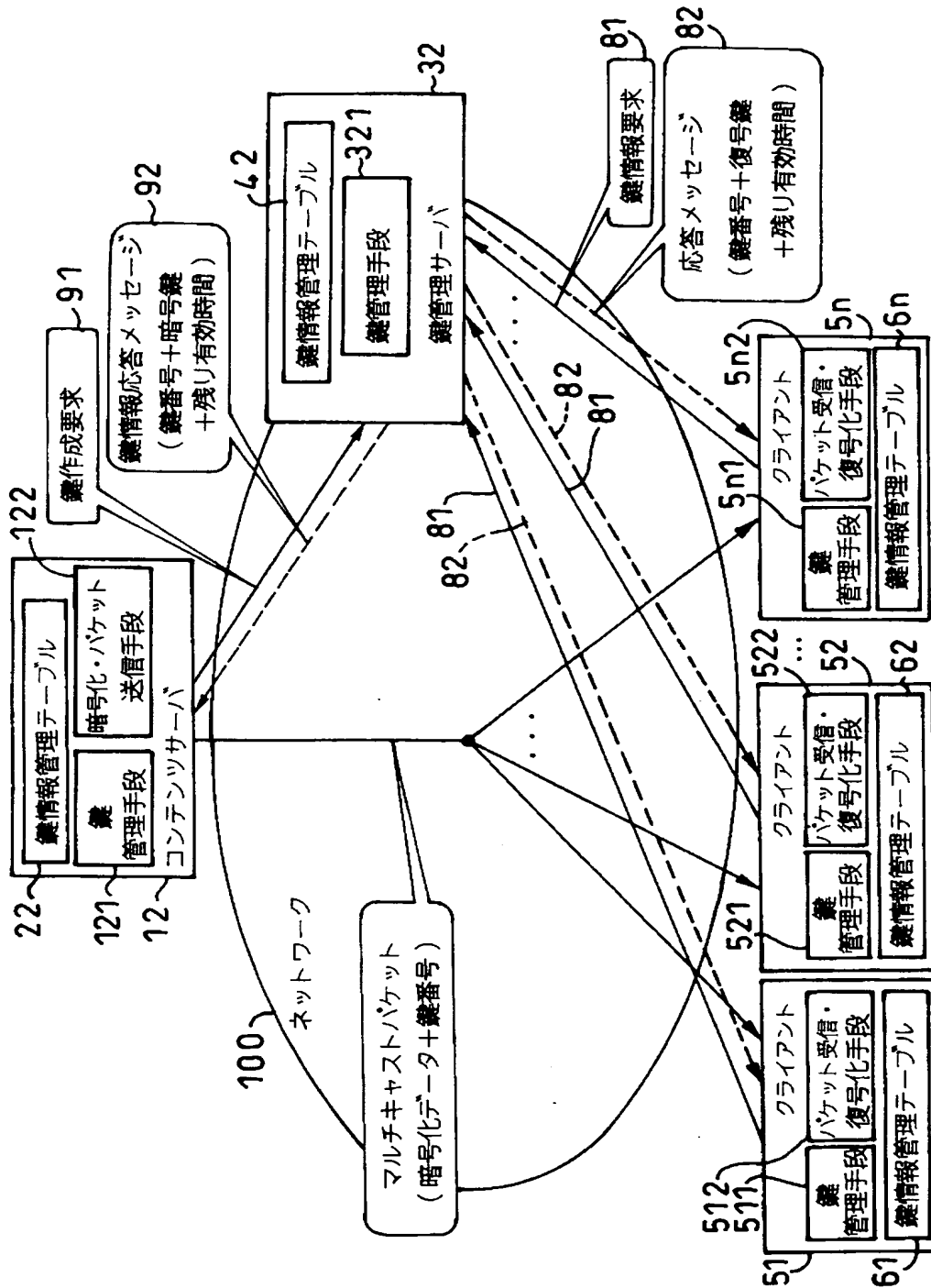
【図 5】



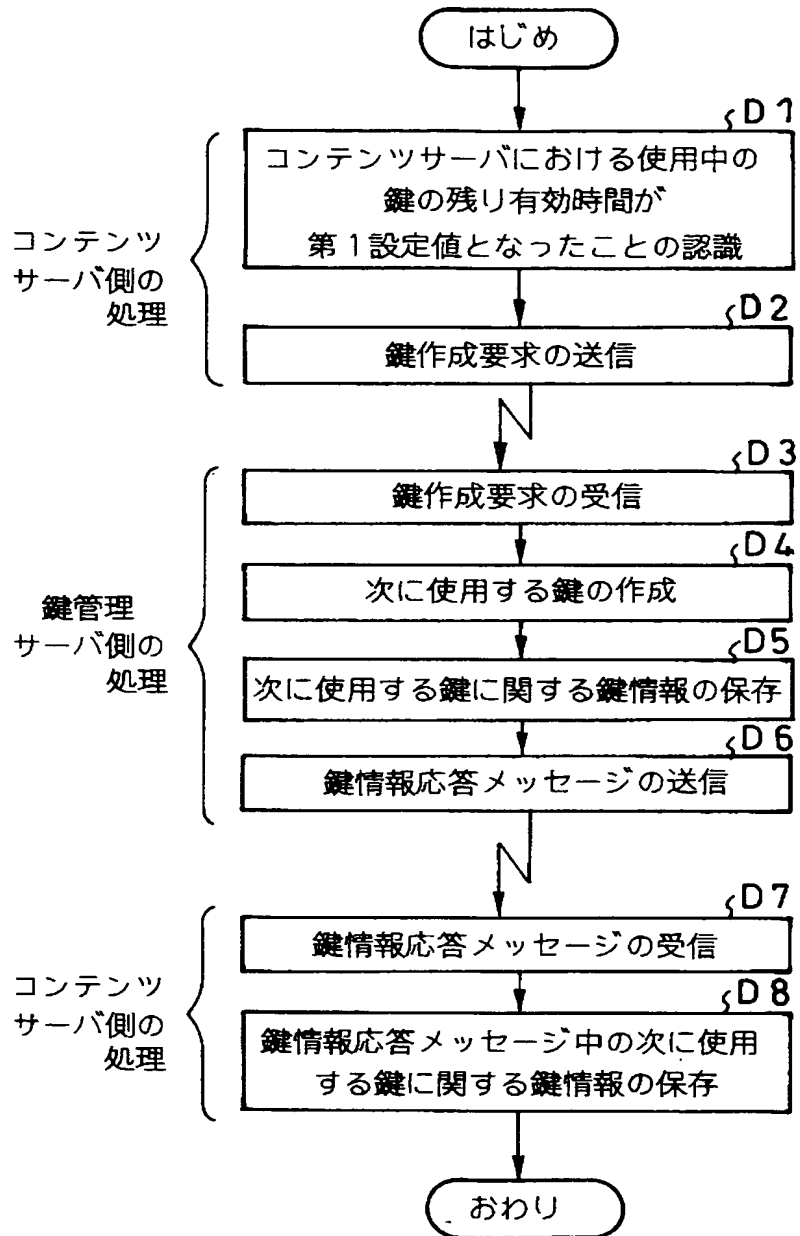
【図 6】



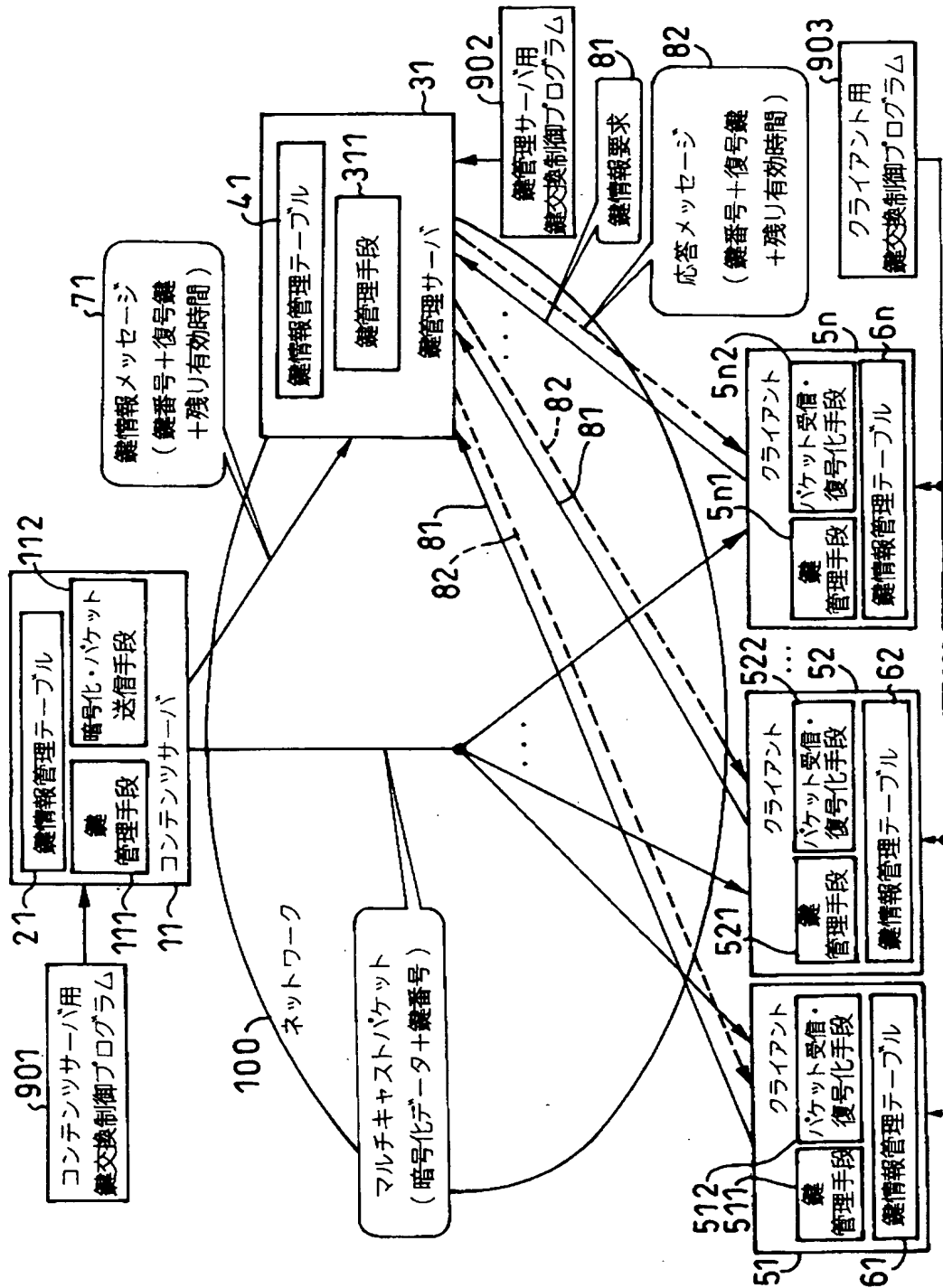
【図 7】



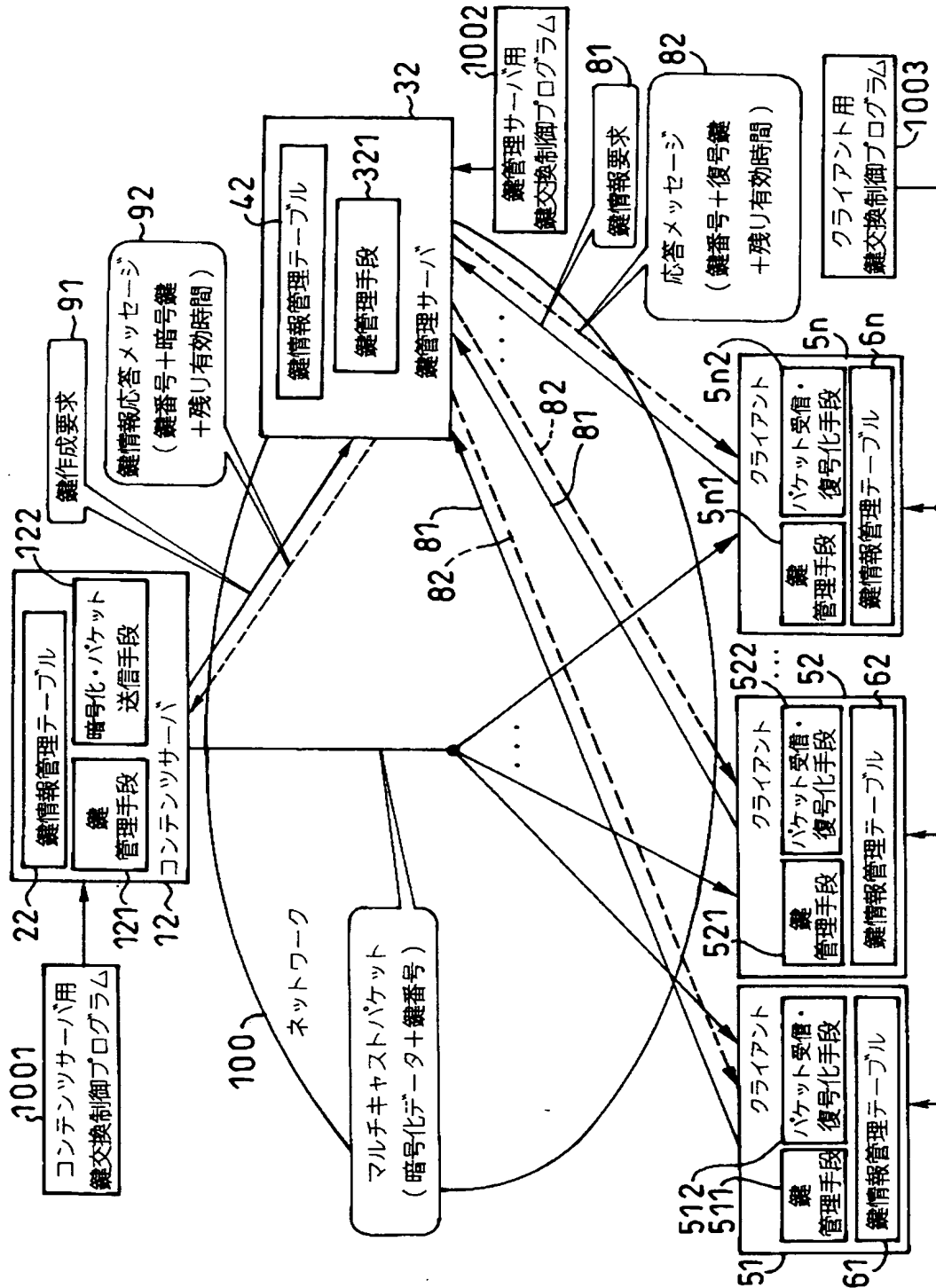
【図 8】



【図 9】



【図 10】



【書類名】 要約書

【要約】

【課題】 鍵変更（交換）時に、新しい復号鍵をクライアントが取得するために生じる処理の遅延を回避する。

【解決手段】 コンテンツサーバ 1 1 は、使用中の鍵の有効時間内に次に使用する復号鍵を鍵管理サーバ 3 1 に配布し、鍵番号を含むマルチキャストパケットを送信する。各クライアント 5 1 ～ 5 n は、使用中の鍵の有効時間内であってコンテンツサーバ 1 1 が鍵管理サーバ 3 1 に次に使用する復号鍵を配布した後の時点に、鍵管理サーバ 3 1 に対して当該次に使用する復号鍵の送付を要求する。また、マルチキャストパケット中の鍵番号に対応する復号鍵により当該マルチキャストパケット中の暗号化データの復号化を行う。鍵管理サーバ 3 1 は、コンテンツサーバ 1 1 から次に使用する復号鍵を受け取り、各クライアント 5 1 ～ 5 n からの送付要求に応じて当該次に使用する復号鍵をその要求元に送信する。

【選択図】 図 1

認定・付加情報

特許出願の番号	特願 2 0 0 2 - 3 3 2 4 0 4
受付番号	5 0 2 0 1 7 3 1 5 2 6
書類名	特許願
担当官	第八担当上席 0 0 9 7
作成日	平成 1 4 年 1 1 月 1 8 日

< 認定情報・付加情報 >

【提出日】	平成14年11月15日
-------	-------------

次頁無

特願 2 0 0 2 - 3 3 2 4 0 4

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 4 2 3 7]

1. 変更年月日

1 9 9 0 年 8 月 2 9 日

[変更理由]

新規登録

住 所

東京都港区芝五丁目 7 番 1 号

氏 名

日本電気株式会社

特願 2 0 0 2 - 3 3 2 4 0 4

出 願 人 履 歴 情 報

識別番号

[0 0 0 2 3 2 2 5 4]

1. 変更年月日

1 9 9 0 年 8 月 3 0 日

[変更理由]

新規登録

住 所

東京都港区三田 1 丁目 4 番 2 8 号

氏 名

日本電気通信システム株式会社